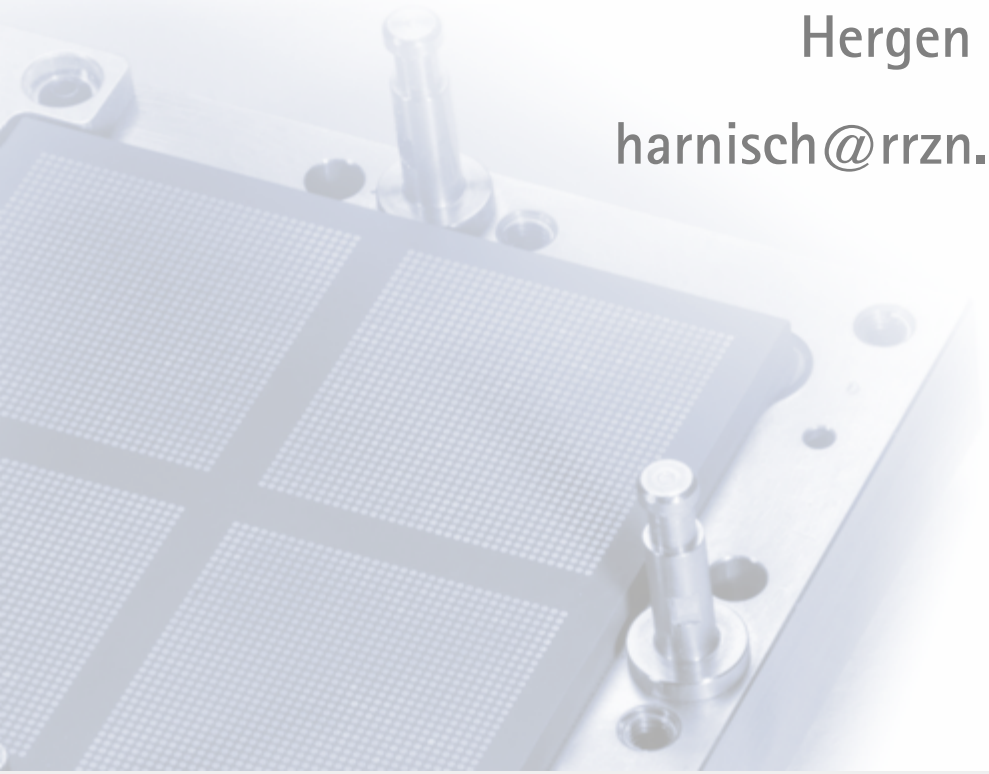
Begrüßung & zur Sicherheitslage



Hergen Harnisch

harnisch@rrzn.uni-hannover.de

Programm

Dienstag 19.05.09

09:15-09:45 Sicherheitslage
09:45-10:45 Client-Absicherung
10:45-11:15 *Pause*
11:15-12:45 Umgang mit Infektionen

Montag 10.08.09 / Dienstag 11.08.09

10.08. Personal-Firewall
10.08. Mac-OS-X: Firewalling etc.
11.08. Samba
11.08. Datenträger-Verschlüsselung

1 Angriffslage

2 Conficker:

- Überblick
- Wurm-Eigenschaft
- andere Verbreitungswege
- Update- & Payload-Download
- Aufspüren
- Verbreitung
- Zusammenfassung

3 Torpig/Mebroot

Überblick

meist Server-Hacks oder Social-Engineering

… wie schon mehrfach hier erwähnt:

- eigentlich kaum noch Würmer, Viren
- stattdessen nachwievor direkte Hacks Webserver & SSH-Bruteforce
- und vor allem „client-seitig initiierte“ Malware-Hacks
- stetige Zunahme von Stealth-/Rootkit-Funktionen in der Malware

Conficker-Wurm

Seit längerer Zeit mal wieder ein echter Wurm, der Schwachstellen in Windows-Ports für RPC/Freigaben (TCP 139, TCP 445) nutzt.

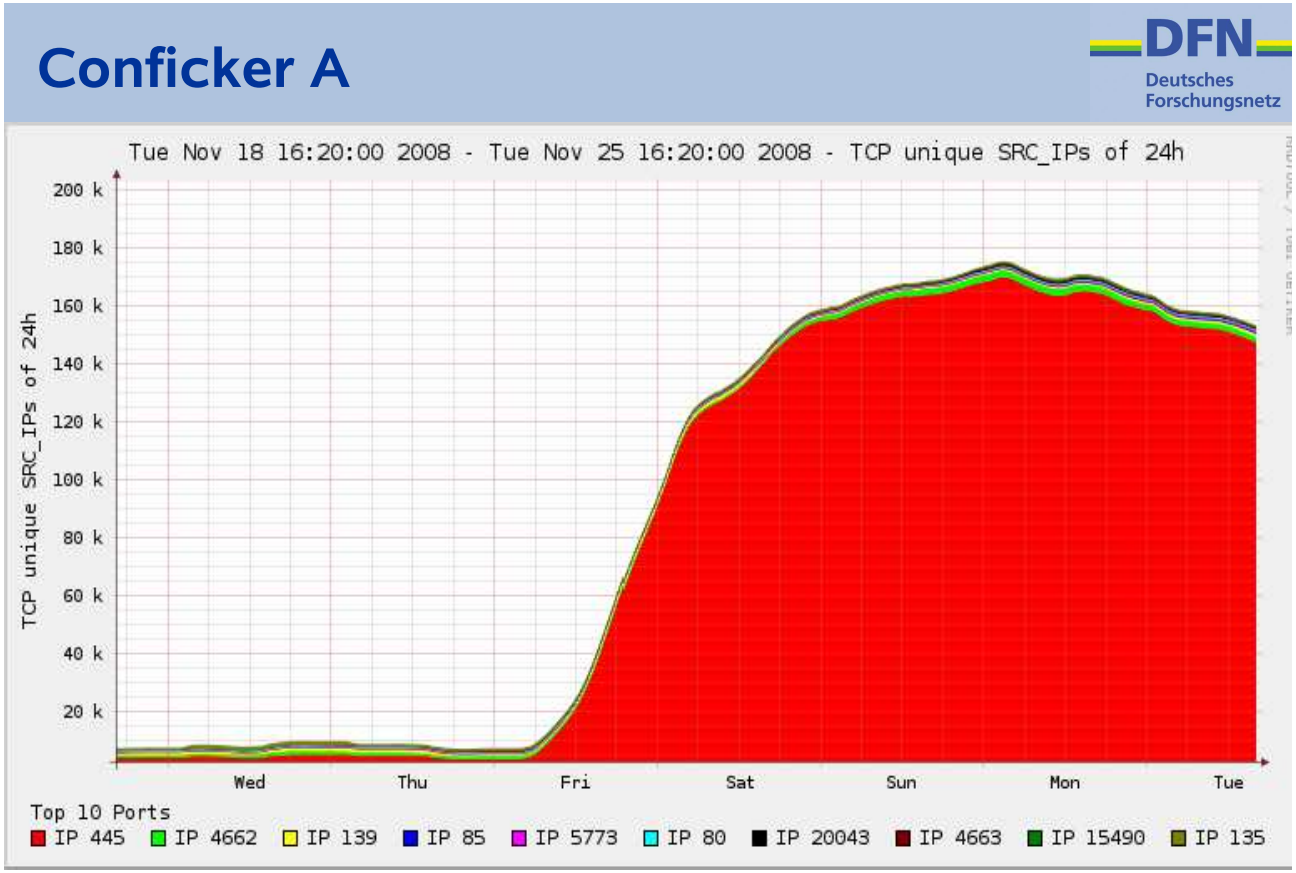
Conficker: Überblick

Namen und Versionen

TA08-297A (other)
CVE-2008-4250 (other)
VU827267 (other)
Win32/Conficker.A (CA)
Mal/Conficker-A (Sophos)
Trojan.Win32.Agent.bccs (Kaspersky)
W32.Downadup.B (Symantec)
Trojan-Downloader.Win32.Agent.aqfw (Kaspersky)
W32/Conficker.worm (McAfee)
Trojan:Win32/Conficker!corrupt (Microsoft)
W32.Downadup (Symantec)
WORM_DOWNAD (Trend Micro)
Confickr (other)

Conficker-A seit 21.11.2008
Conficker-B seit 29.12.2008
Conficker-C seit 20.02.2009
Conficker-D seit 04.03.2009
Conficker-E seit 08.04.2009

Conficker: Wurm-Eigenschaft



Quelle: Carmentis 25.11.2008

Sprunghafte Zunahme von 445-Scans im Internet ⇝ Malware/Wurm!

Conficker: Wurm-Eigenschaft

Microsoft-Sicherheitslücke

Beschrieben in:

- Microsoft Security Bulletin MS08-067
- Knowledge-Base-Artikel KB958644

- Angriff über TCP-Port 445
  Anfällig: RPC-DCOM (Datei- & Druckerfreigabe / Browserdienst)
- Gefährdung unterschiedlich:
  $\leq$ XP/2003 generell bei Porterreichbarkeit
  Vista/2008 nur nach Authentifizierung
- Lücke & Patch veröffentlicht am 23.10.08, Conficker kam 21.11.08;
  Malware-Kit bereits seit 9/2008, Gimmev-Wurm seit 9-10/2008

Sophos-Studie vom 10.04.09: 10% aller PCs noch ungepatcht

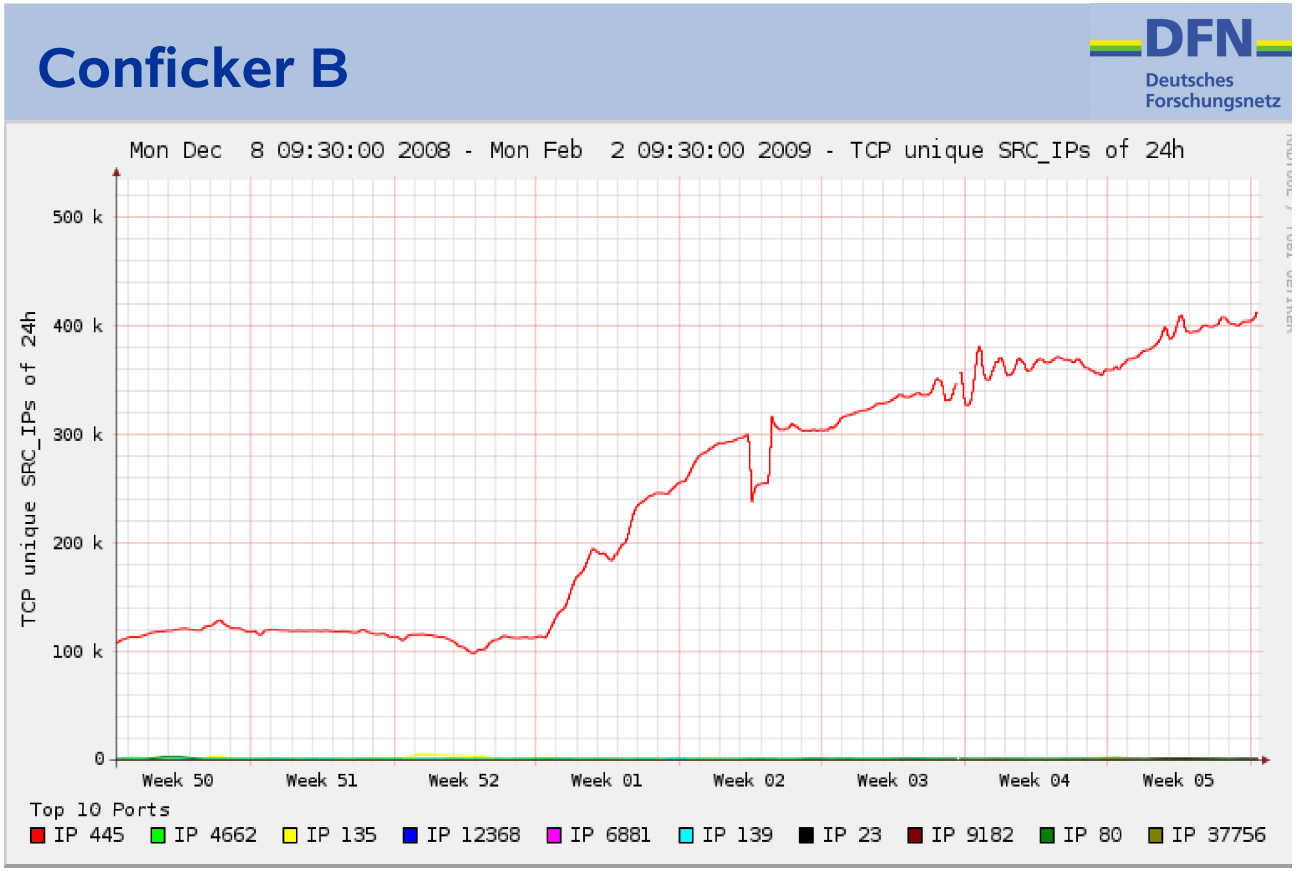
R|R|Z|N

Bedrohungspotential

Die Sicherheitslücke im RPC-Dienst wird über das Netz ausgenutzt.

- Firewalls und die im LUH-Netz vorgenommene Sperrung der „Windows-Ports“ in allen Routern verhindert Infektion aus dem Internet oder aus anderen Einrichtungen der Uni.
  `http://www.rrzn.uni-hannover.de/portsperren.html`
- Daher meist Infektionen über das Netz
  - von Privatrechnern (ohne DSL-Router),
  - vieler Rechner in einem LAN.
- Anfällig sind ungepatchte Systeme, daher besonders gefährdet
  - Privatrechner
  - zentral administrierte PCs mit Tests vor Patch-Rollout

Conficker: andere Verbreitungswege



Quelle: Carmentis 02.02.2009

erneuter Anstieg ⇝ neuer Verbreitungsweg!

Conficker: andere Verbreitungswege

Neben der automatischen Weiterverbreitung eines Wurms nutzt Conficker seit Conficker.B (Ende 2009) auch traditionelle Viren-Wege:

Medien/USB über USB-Memorysticks und andere mobile Datenträger nicht nur über Datei-Infektion sondern vorallem *AutoRun*-Funktionalität

Freigaben ein infizierter Rechner durchsucht verbundene Netzwerkfreigaben und infiziert dort befindliche Dateien. Auch Mount-Versuche mit Passwort-Raten und aktiven Accounts.

$\longrightarrow$ Rechner, die `AutoRun.Inf` beachten oder infizierte Dateien ausführen, werden infiziert.

Conficker: Update- & Payload-Download

Conficker lädt Updates und Payload (ab bestimmtem Datum) nach:

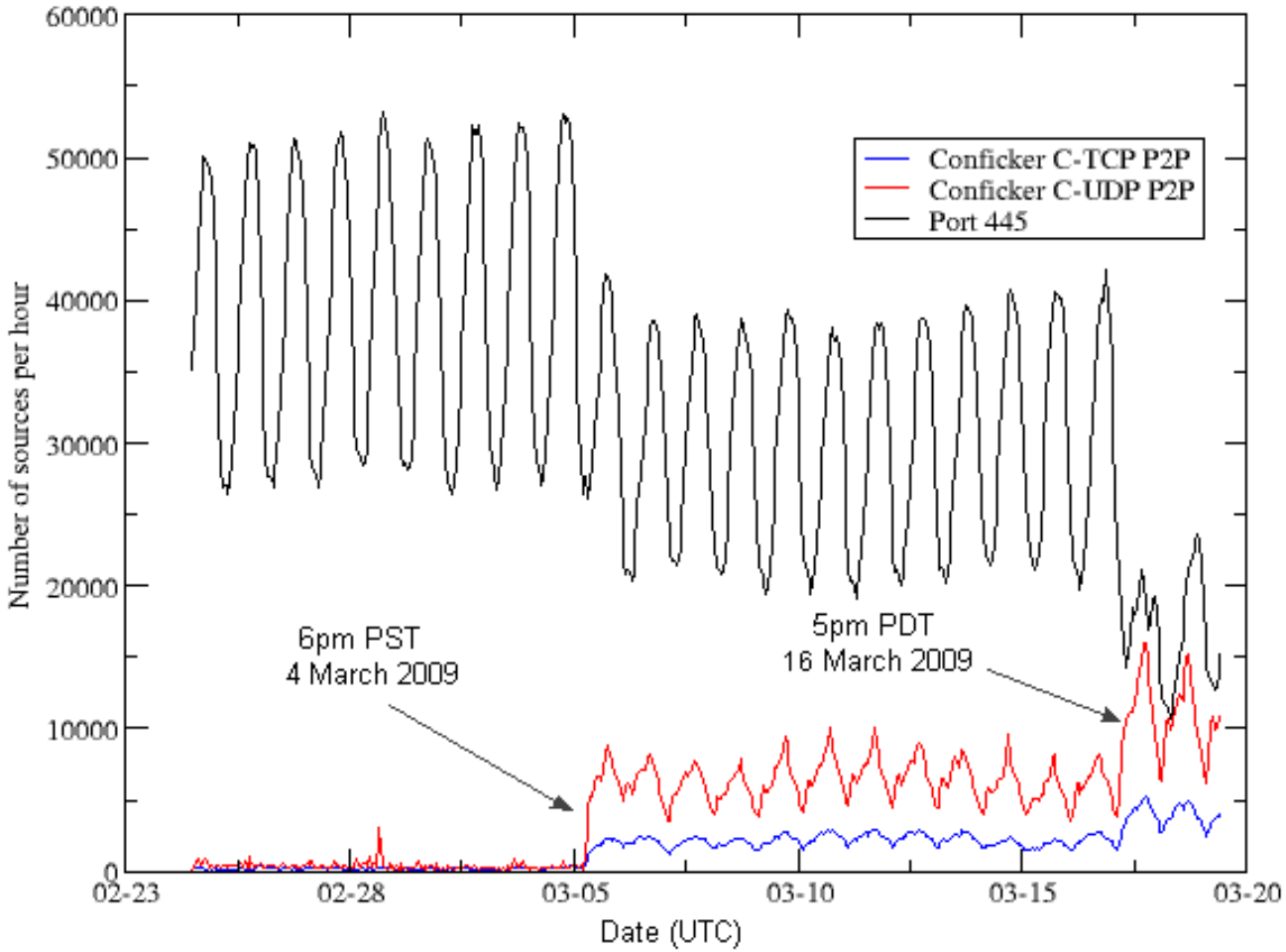
- Pro Tag wird eine Liste von Domainnamen berechnet
- und per Zufall ein Teil dieser Domains abgefragt.

(domain flux)

Zudem aber seit 20.02.2009 auch Updates über P2P.

Variante	Entdeckung	Update seit	TLDs	Domains/Tag
A	21.11.08	25.11.09	5	250
B	29.12.08	01.01.09	8	250
C	20.02.08	01.04.09	110	500 aus 50.000
C-E		20.2.09	via P2P statt DNS	

Conficker: Update- & Payload-Download



Umstellung auf P2P in verschiedenen Varianten ist erkennbar

Quelle Grafik: `http://mtc.sri.com/`.

Conficker: Aufspüren

R|R|Z|N

Conficker-infizierte PCs kann man finden durch:

- Scan auf dem Host, insbesondere mit
  - Zugriff auf durch Conficker gesperrte Webseiten, vgl.
    http://four.cs.uni-bonn.de/fileadmin/user_upload/leder/cfdetector/

    http://www.confickerworkinggroup.org/infection_test/cfeyechart.html
  - speziellen Conficker-Tools
  - MSRT[1] erkennt Conficker A&B seit 15.1.2009
- Scan des LANs (Abscannen aller Rechner) nach
  - Lücken in der RPC-Implementation (ungepatcht)
  - IP-abhängigen Portöffnungen der P2P-Implementation
- ausgehenden Scans auf Zielport TCP-445
  - in Firewall- & Router-Logs
  - aufschlagende in Darknets (z.B. des DFN)

[1] Malicious Software Removal Tool von Microsoft, automatisch per Update

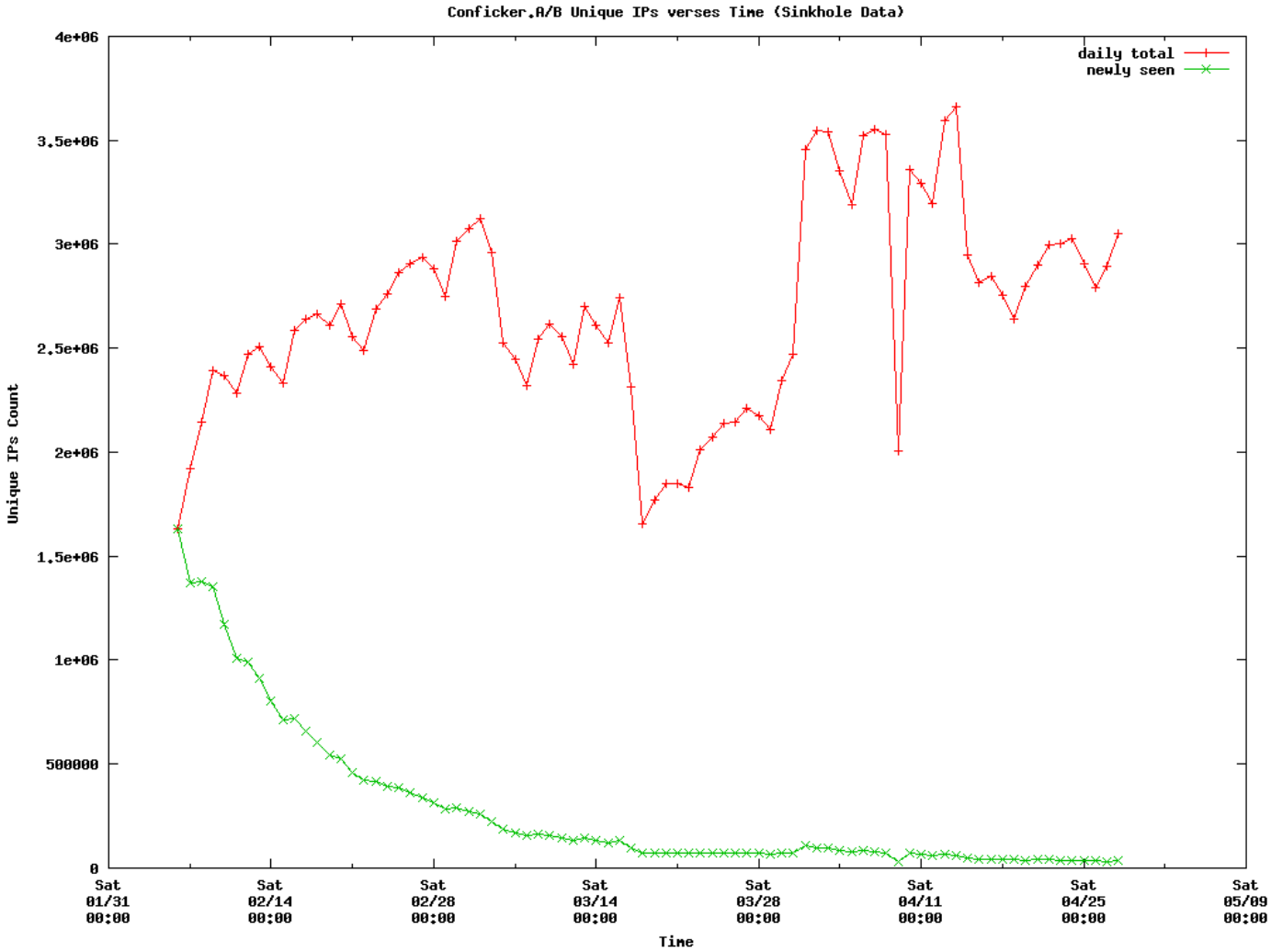
Conficker: Aufspüren

DNS

Conficker fragt zufällig 250 Domains aus einer tagesabhängig berechneten Grundmenge von 250+250+50.000 (A+B+C) ab.

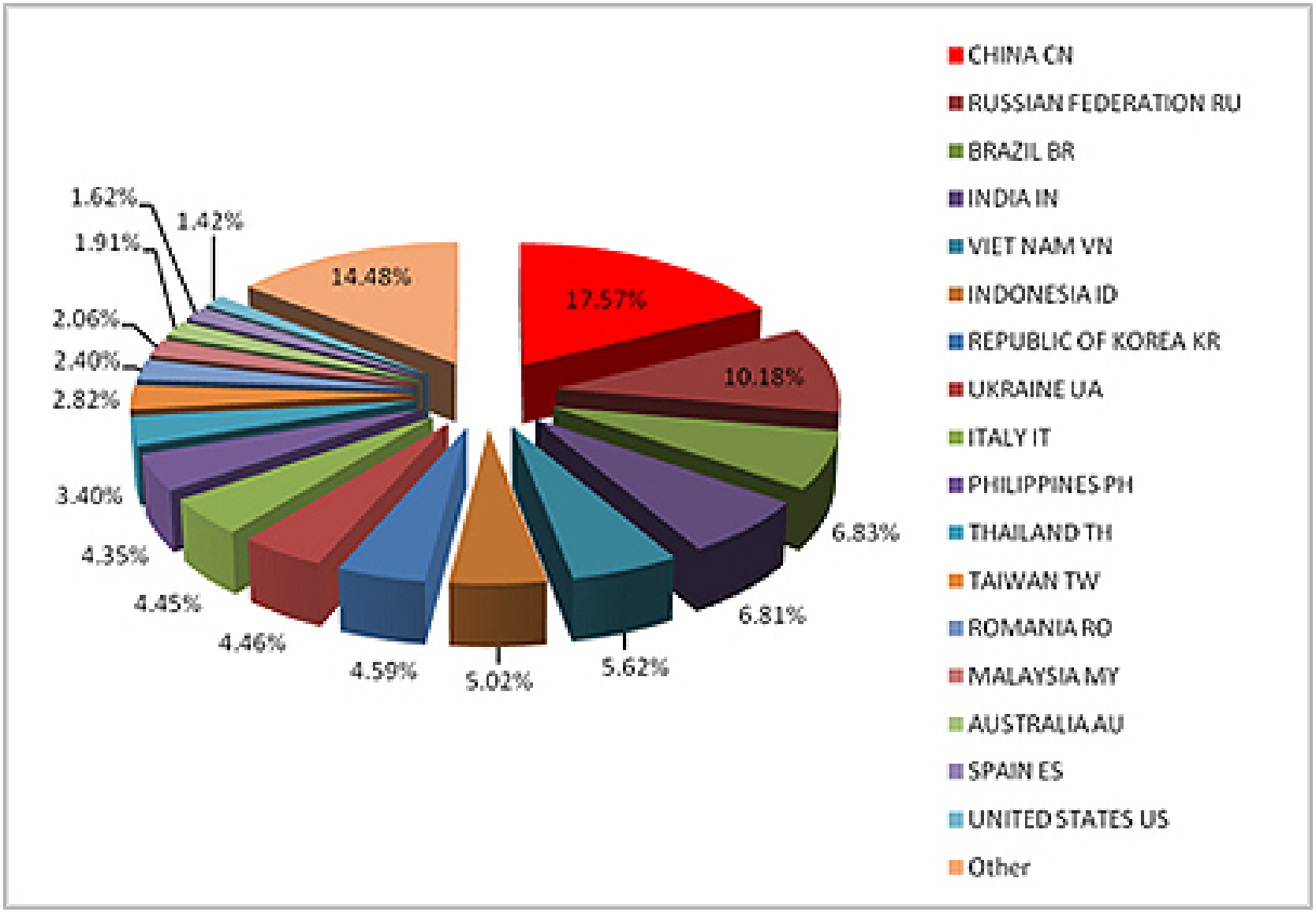
- Conficker-Working-Group beantragte Teil dieser Domains
- bei A+B konnten die Domains als „Dummy“ auf eigenen DNS-Resolvern eingerichtet werden, dann Log-Auswertung oder Umlenkung auf eigene loggende Seite
- an der LUH seit 1.4.2009 aktiv:
  - jede Client-Anfrage wird durch Bind-Server (kurzfristig) geloggt
  - Python-Skript wertet Logs aus und vergleicht mit Einträgen in Berkeley-Datenbank-Datei, die vorberechnete Conficker-Domainnamen enthält
  - Matches werden wirklich und längerfristig geloggt
  - viele Matches einer IP zu verschiedenen Domains $\Longrightarrow$ Conficker-Infektion (eine Domain reicht nicht, könnte echte sein)

Conficker: Verbreitung



Verlauf im Zeitraum 15.2.-3.5. (Mitigation Conficker-Working-Group, d.h. DNS-Hits; CWG)

Conficker: Verbreitung



überwiegend in Asien, Stand 13.4.2009; Quelle: BKIS Vietnam

Conficker: Verbreitung

R|R|Z|N

im Internet

Conficker-Working-Group (Schätzung vom 14.04.2009):
Conficker A+B 3.4 Millionen IPs Conficker C 1.2 Millionen IPs Kaspersky (15.04.2009): 200.652 IPs in 24h im P2P-Netz

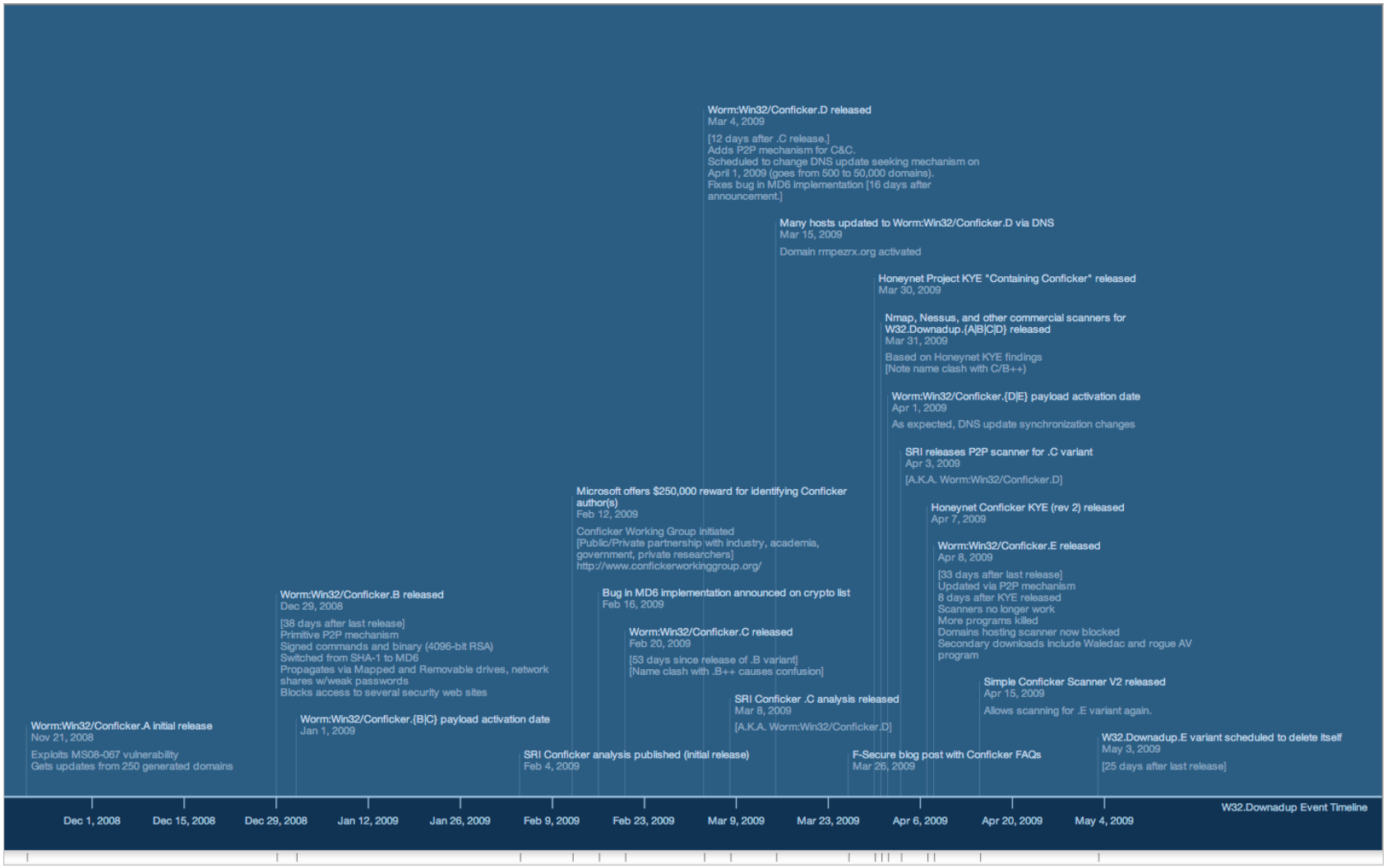
im LUH-Netz

DNS-Überwachung seit 1.4.2009:

- ca. 4 IPs pro Tag, nur wenig abnehmend
- meist Conficker-B, selten C, noch seltener A
- kaum in Einrichtungen/Instituten, fast nur Wohnheime & WLAN
- auch in LANs mit Infektionen keine Masseninfektionen

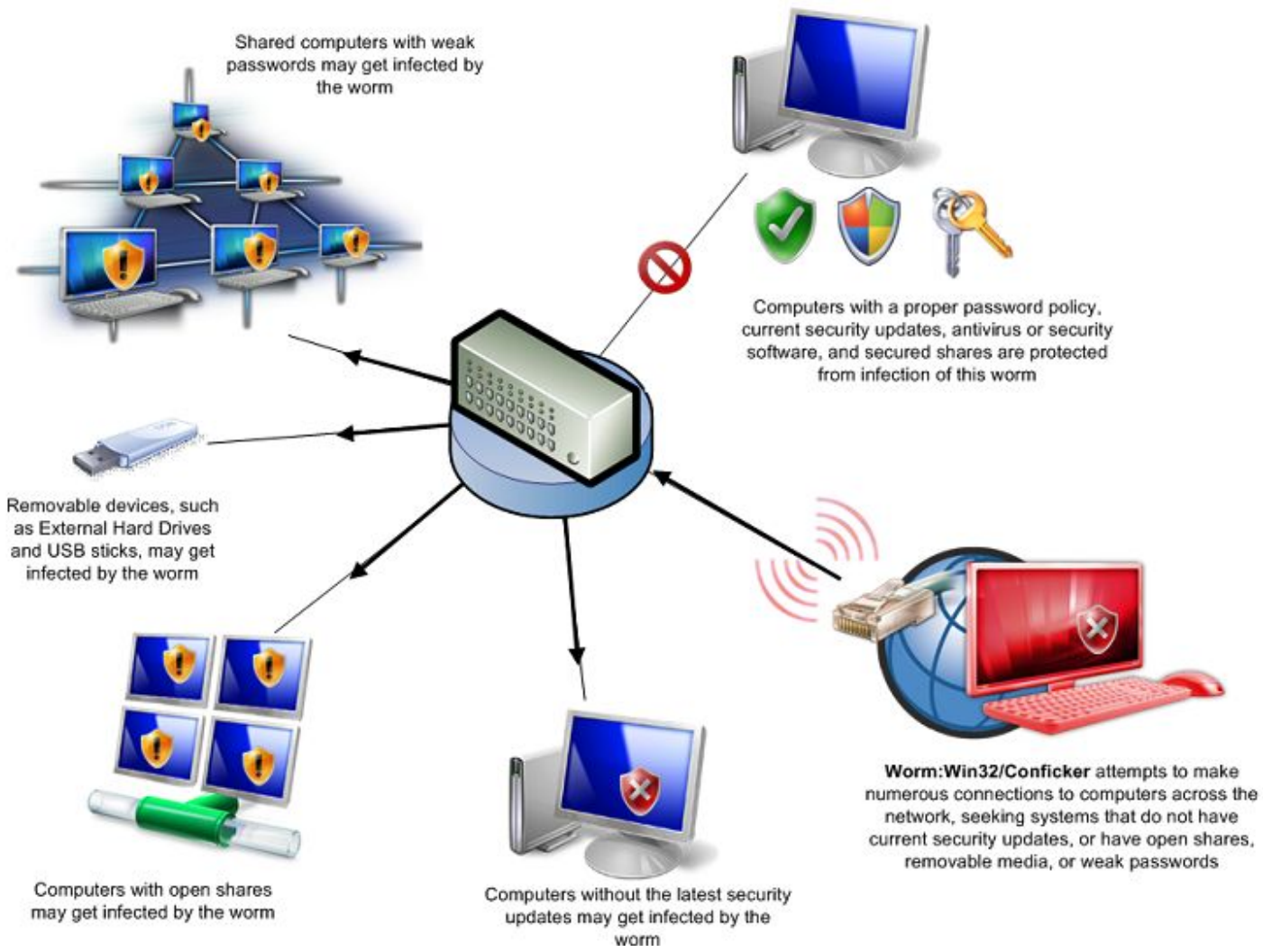
aber: Conficker-C nutzt DNS nicht mehr, eher P2P (Scan ausstehend)

Conficker: Zusammenfassung



Quelle: Conficker-Working-Group (http://www.confickerworkinggroup.org/)

Conficker: Zusammenfassung



Quelle: Microsoft

Torpig/Mebroot

Torpig Botnet-Agent, wird installiert durch Trojaner

Mebroot Rootkit, verschleiert Existenz von Torpig

- Torpig und Mebroot treten meist in Verbindung auf
- Infektion häufig durch *drive by download*
- Botnet dient hauptsächlich dem Diebstahl von Passwörtern und Zugangskennungen
- nicht im infizierten System zu finden,
  - weder durch Virenscanner
  - noch durch Anti-Rootkits

(Anti-Rootkit Radix soll das inzwischen können)

Mebroot

- setzt sich (u.A.) in den Master-Boot-Record („MBR-Rootkit“)
- im Bootprozess wird ein Hook zur Rootkit/Payload-Aktivierung in die Windows-Initialisierung geschrieben – die Initialisierungsroutine ist später aber überschrieben und somit unauffindbar
- Rootkit und zugehörige Daten sind nicht in Dateien abgelegt, sondern direkt in bestimmten Sektoren der Platte
- nur der MBR muss vor dem laufenden Windows versteckt werden $\longrightarrow$ dafür sind nur 2 DWORDS in `driver.sys` verändert
- der MBR ist der Rootkit-Startpunkt, Registry-Anpassung o.Ä. sind nicht nötig

„This malware is very professionally written and produced. Which of course means itś not written for fun.“ (F-Secure)

Aufspüren

Botnet-Übernahme

UCSB konnte Anfang 2009 das Botnet für 10 Tage übernehmen

- lieferte Interna zum Verständnis
- und Daten über (zu dem Zeitpunkt) infizierte Hosts

`http://www.cs.ucsb.edu/~seclab/projects/torpig/index.html`

DNS verwendet wie Conficker *domain flux*, benutzt dabei aber nicht verhersagbare Zusatzdaten (per URL-Download die Twitter-Suchtrends vor 2 oder 3 Tagen)

$\longrightarrow$ Log-Filterung auf DNS-Servern im Prinzip möglich

Scan Scan an jedem einzelnen Rechner mit

- Radix-Anti-Rootkit im laufenden Windows-System
- mit separaten Boot-Medien & Viren-Scanner