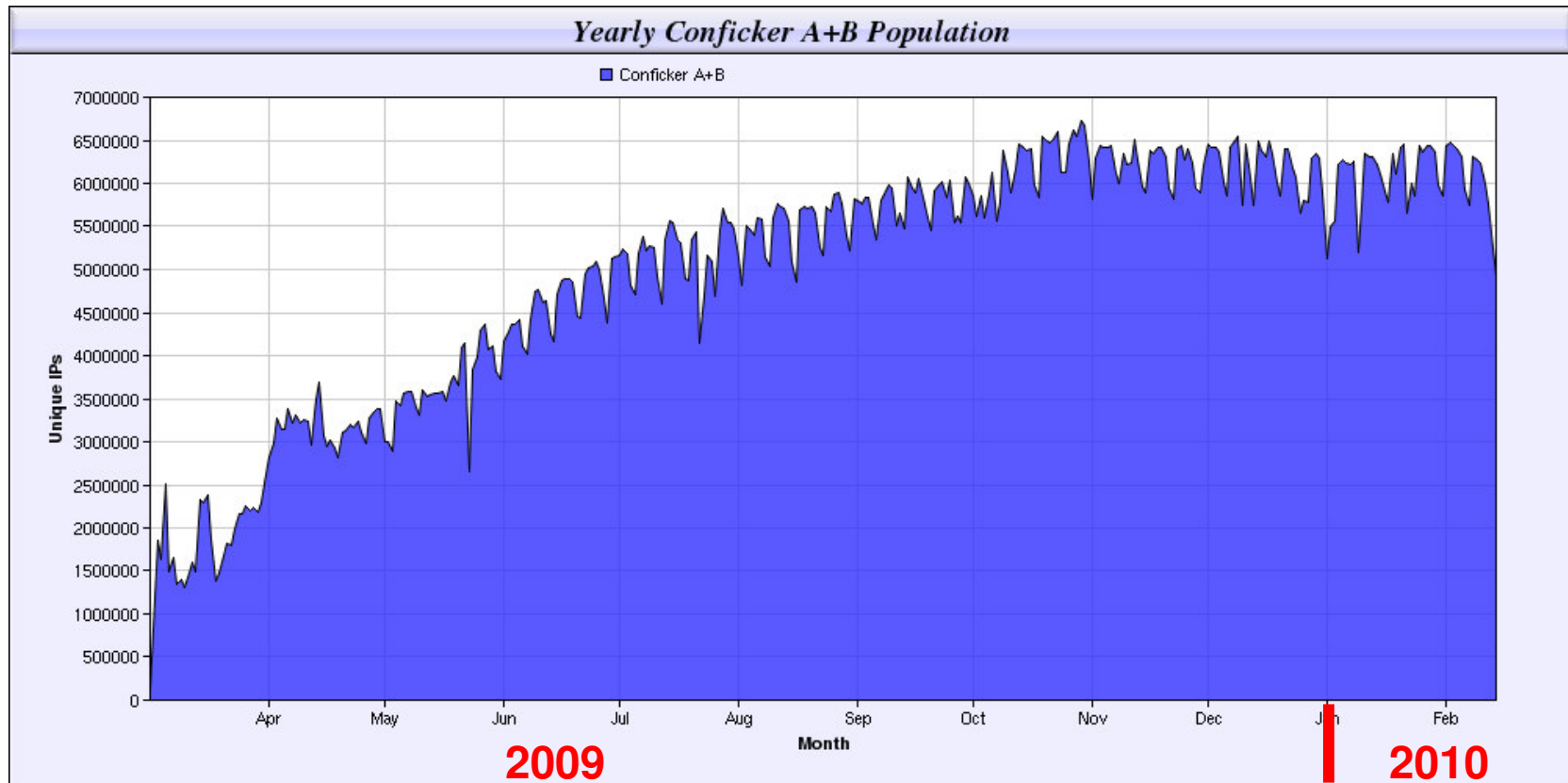
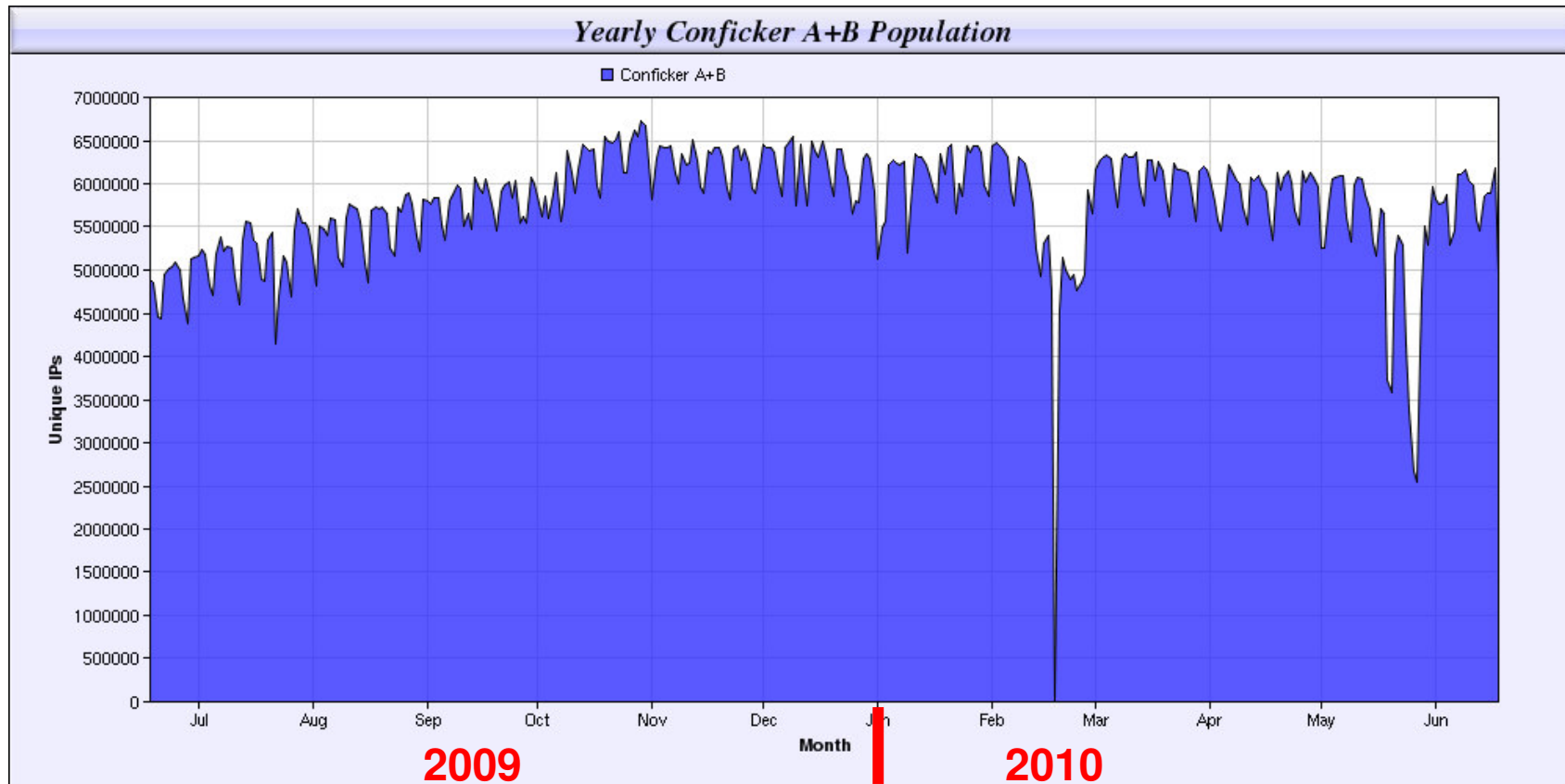


Conficker: Zahl infizierter Systeme



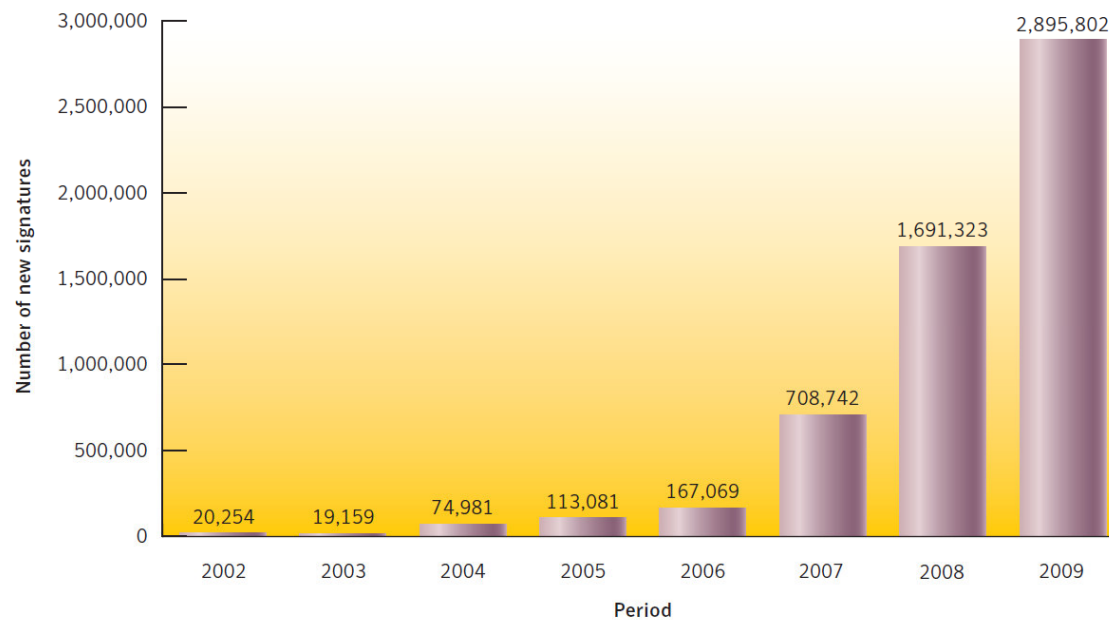
Quelle: <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking>

Conficker: Zahl infizierter Systeme



Quelle: <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking>

Cyber Defense – Vielfalt der Schadprogramme



2009: Neue Schad-Codes
~ 8.000 pro Tag
~ 330 pro Stunde
~ 5 pro Minute

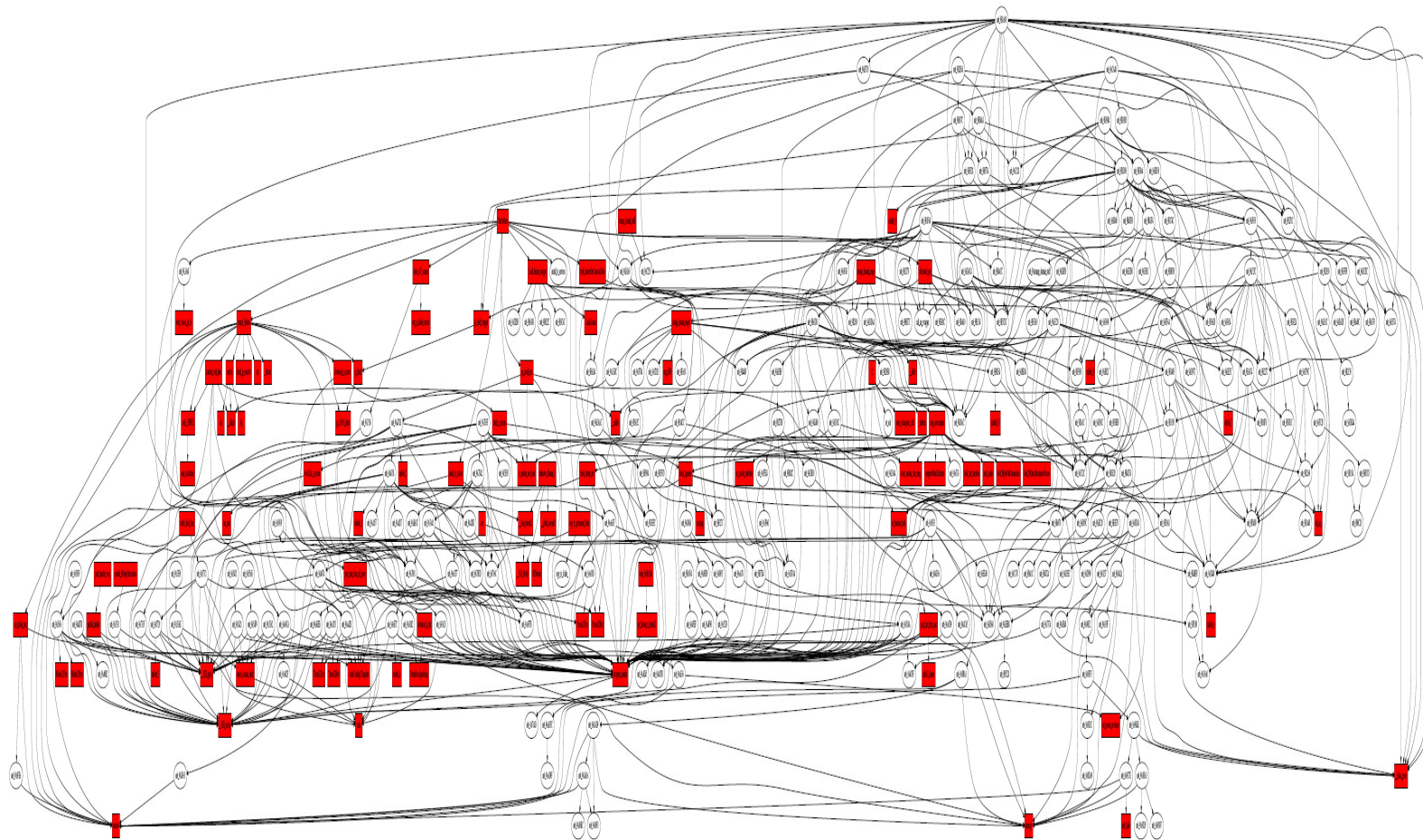
➔ **Viren-Scanner bieten kaum noch Schutz**

Figure 10. New malicious code signatures

Source: Symantec.

Quelle: Symantec Global Internet Security Threat Report Trends for 2009
Volume XIV, Published April 2010

Struktur des Conficker-Wurms



Conficker: Looking for Updates since April 1, 2009

```
lea    eax, [ebp+12Ch+SystemTime]
push  eax    ; lpSystemTime
call  ebx ; GetLocalTime
cmp   [ebp+12Ch+SystemTime.wYear], 2009
ja    short loc_9A3C37
```

•Compare: Year, 2009

```
jnz   short loc_9A3C4D
```

```
cmp   [ebp+12Ch+SystemTime.wMonth], 4
ja    short loc_9A3C37
```

•Compare: Month, 4

```
jnz   short loc_9A3C4D
```

```
cmp   [ebp+12Ch+SystemTime.wDay], 1
jb    short loc_9A3C4D
```

•Compare: Day, 1

```
loc_9A3C37:
cmp   [ebp+12Ch+var_19C], 0
jz    short loc_9A3C46
```

```
call  sub_9B36E8
test  eax, eax
jnz   short loc_9A3C4D
```

```
loc_9A3C46:
call  update_requests
mov  esi, eax
```

•Request Updates