

**[SECURE]**  
Business Austria  
Kompetenz für Wissenschaft und Industrie.

**Trends in Forschung und  
Entwicklung der IT-Sicherheit**

**Markus Klemen**  
Secure Business Austria

© 2014-2015 Secure Business Austria

**[SECURE]**  
Business Austria  
Kompetenz für Wissenschaft und Industrie.

**Inhalt**

- Über Secure Business Austria
- Aktuelle Forschungs- und Entwicklungsgebiete
- Forschungsschwerpunkt: Malicious Code Detection

© 2014-2015 Secure Business Austria

**Secure Business Austria** **[SECURE]**  
Business Austria  
Kompetenz für Wissenschaft und Industrie.

- Industrielles Kompetenzzentrum (K-Ind) für IT-Sicherheit
- Schnittstelle zwischen Universitäten und Wirtschaft
- TU Wien, TU Graz, Universität Wien
- Angewandte Sicherheitsforschung für und mit industriellen Partner
- Rund 35 vollzeitäquivalente Mitarbeiter
- Gefördert von BMWA und Stadt Wien

© 2014-2015 Secure Business Austria

**[SECURE]**  
Business Austria  
Kompetenz für Wissenschaft und Industrie.

**Forschungsschwerpunkte**

*Im organisatorischen Bereich:*

- Kosten/Nutzen Analyse von IT-Sicherheit
- Risikomanagement
- Security Awareness für Mitarbeiter
  - OCG IT-Security Zertifikat
- Prozesssicherheit
  - Secure Workflows

© 2014-2015 Secure Business Austria

**Forschungsschwerpunkte** **[SECURE]**  
Business Austria  
Kompetenz für Wissenschaft und Industrie.

*Im technischen Bereich:*

- Malicious Code Detection
- Fraud Detection
- Privacy in Medical Environments
- Cryptochip Tampering
  - Differential Fault Analysis

© 2014-2015 Secure Business Austria

**[SECURE]**  
Business Austria  
Kompetenz für Wissenschaft und Industrie.

**Security Trends**

- Sicherheit in komplexen Systeme
- Sicherheit für InterOp
- Problembereich NGN / Infrastruktursicherheit
- Neue Herausforderungen durch Virtualisierung
- Anti-Spam / Antivirentechnologien
- Mobile Security
- NAP/NAC
- Web Application Firewall

© 2014-2015 Secure Business Austria

## Next Generation Networks

- VoIP Konvergenz
- „Alles über ein Netz“
- Abhängigkeiten
  - von wenigen Anbietern (analog zu Google, Skype, ...)
  - von Netzwerk und Strom
    - Mobilfunk teilweise redundant (last mile), aber ebenfalls Einbindung in NGN.
  - Beispiel Notfallhandbücher online

[7]

© 2014 2015 Secure Business Austria

## Virtualisierung

- AV Spezialisten setzen massiv auf VM
  - Erkennung von virtuellen Umgebungen durch Schadsoftware
  - Probleme für Anti-Virenhersteller
- VM Rootkits
  - Einnehmen von Hostsystemen
  - Stichwort Blue Pill
  - Auf Guest-Ebene nicht erkennbar

[8]

© 2014 2015 Secure Business Austria

## Anti-Spam

- Traditionelle Ansätze
  - Biometrieproblem
- Radikal neue Ansätze
  - Oftmals Akzeptanzprobleme
  - Noch einige Detailprobleme
  - Lösen nur Symptome, nicht die Ursache
- Langfristige Lösung: „Mail-PKI“

[9]

© 2014 2015 Secure Business Austria

## Malicious Code Detection

### Herausforderungen:

- Trojaner werden immer raffinierter
- Massive Investments durch Organisierte Kriminalität
  - Direkte Attacken auf Zieluser
  - Plattformen für Spamming (Botnetze)
- Neue Paradigmen durch Virtualisierung
  - Stichwort Blue Pill
  - Probleme der Erkennung virtueller Umgebungen durch Schädlinge

[10]

© 2014 2015 Secure Business Austria

## Malicious Code Detection

### Drei technische Ansätze:

- Signaturbasierte Ansätze
- Dynamische Codeanalyse („Heuristik“)
- Statische Codeanalyse

[11]

© 2014 2015 Secure Business Austria

## Malicious Code Detection

### Signaturbasierte Ansätze:

- Zahl der Schädlinge wird unüberschaubar
- Veraltete Signaturen müssen oft weggelassen werden
- Zusehends Performanceprobleme
- Kleine Programmänderungen (Code Generators) können bereits neue Signatur erforderlich machen
- Gefahr, dass systemrelevante Dateien als gefährlich erkannt werden

[12]

© 2014 2015 Secure Business Austria

## Malicious Code Detection

### Dynamische Codeanalyse:

- Kompilierter Code läuft in Sandbox ab und wird beobachtet
- Sehr ausführliche Reports
- Relativ schnell und einfach zu testen
- Nachteile:
  - Virtuelle Umgebungen können erkannt werden, Schädling bleibt inaktiv
  - Es kann nicht vollständig aufgeklärt werden, was der Code wirklich macht

[13]

## Malicious Code Detection

### Statische Codeanalyse:

- Programmcode wird nicht ausgeführt, sondern statisch analysiert
- Alle möglichen Verzweigungen werden analysiert
- Nachteile:
  - Analyse ohne Quellcodes schwierig
  - Forschung im Codeentwicklungsbereich etabliert, für Malware Detection noch kaum genutzt

[14]

## Pathfinder (Codename ANUBIS)

- ANalyzing Unkown BinarieS
  - Public Version: <http://anubis.seclab.tuwien.ac.at/>
  - Automatisierte Analyse von Malware Detailreports
  - Weltweit nur zwei vergleichbare Systeme
  - Durch Sandbox Technik wird Malware in definiertem Environment ausgeführt und beobachtet. Analyse wird in Report beschrieben
  - Memory/Data Tainting Technologie in Verbindung mit Clustering erlaubt z.B. Identifikation von identischer aber mutierender Malware, obwohl Binaries unterschiedlich sind.
  - ANUBIS ist „leading edge“ Technologie mit immensem Potential



[15]

## Technische Situation von ANUBIS

### Verbreitung und Akzeptanz von ANUBIS

- Gute Kritik in div. Internet Foren
- Referenzen auf ANUBIS Reports werden in Mailing Listen verwendet
- Upload von ca. 2000 Samples pro Tag
- Bisher 254549 unique Samples von ANUBIS erhalten
- Malware Szene hat reagiert (sehr gut)
  - Spezielle ANUBIS Evasion Techniken wurden entwickelt
  - D.h. ANUBIS wurde als Bedrohung für Malwareszene erkannt!

[16]

## Auslastung von ANUBIS

### Year 2007 - Overview

2007	January	February	March	April	May	June	July	August	September	October	November	December	Total
Submissions	0	0	1077	5972	27179	41425	14953	24112	25474	63124	57547	70305	331274
Submissions/day	0	0	34,7	199,1	875,1	1380,8	482,4	777,8	849,1	2036,3	1918,2	2270,5	907,6
Number of Analyzed Samples	0	0	906	1868	14449	29733	18017	18371	18432	45030	44695	34872	210529
Number of Analyzed Samples/day	0	0	31,8	62,3	466,1	991,1	523,1	534,5	614,4	1452,6	1499,6	1124,9	576,9

### Year 2008 - Overview

2008	January	February	March	April	May	June	July	August	September	October	November	December	Total
Submissions	57745	17659	0	0	0	0	0	0	0	0	0	0	75404
Submissions/day	1862,7	552,4	0	0	0	0	0	0	0	0	0	0	1536,9
Number of Analyzed Samples	45970	20104	0	0	0	0	0	0	0	0	0	0	66072
Number of Analyzed Samples/day	1452,2	6336,1	0	0	0	0	0	0	0	0	0	0	1348,6

[17]

## Leistungsfähigkeit von ANUBIS



- Report nach 4-6 min. Analyse
- Mensch bräuchte ca. +1 Woche
- Network Traces verfügbar
- Könnten in IDS Signaturen konvertiert werden
- Erstellung und Vergleichen von Malware Verhaltensprofilen

[18]

## Technische und wissenschaftliche Herausforderungen

- Emulation eines realen Computers
  - Eigenheiten einer echten CPU müssen exakt nachgebildet werden
- Gegenmaßnahmen zur Sandbox-Erkennung
  - Viele verschiedene Möglichkeiten, eine Emulation zu erkennen (z.B. durch undokumentierte Befehle oder Delta in Ausführungszeiten)
- Auswertung der bei der Analyse gesammelten Daten
  - Auswahl/Filtering der für den Report relevanten Informationen

www.secure.austria.at

[19]

© 2014-2020 Secure Business Austria

*Vielen Dank für Ihr Interesse!*

www.secure.austria.at

[20]

© 2014-2020 Secure Business Austria