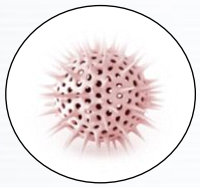
Next Generation Sandboxing

Dokumenten-Scan der neusten Generation

Agenda

- Überblick über die derzeitige Situation
- Prüfungen von E-Mail Anhängen neuster Generation
- Erkennungstechniken auf CPU-Ebene
- Vorbeugende Gefahrenminimierung durch Risiko-Isolierung

Wir befinden uns in einer Welt voller Schwachstellen





SIE müssen sich vor ALLEN schützen…

"ANGREIFER" benötigen nur EINE Schwachstelle





Wie ist die derzeitige Situation?

Warum sehen wir derzeit so viele Angriffsversuche per E-Mail?

Exploit-Kit Angler macht Millionen mit Erpressungs-Trojanern

heise Security 07.10.2015 11:52 Uhr – Daniel AJ Sokolov vorlesen

Cisco hat das Explit Kit Angler in freier Wildbahn studiert und einen Gutteil der Hosts offline nehmen lassen. Wie sich zeigt, haben die Täter ein professionelles System hochgezogen und scheffeln damit richtig Geld.

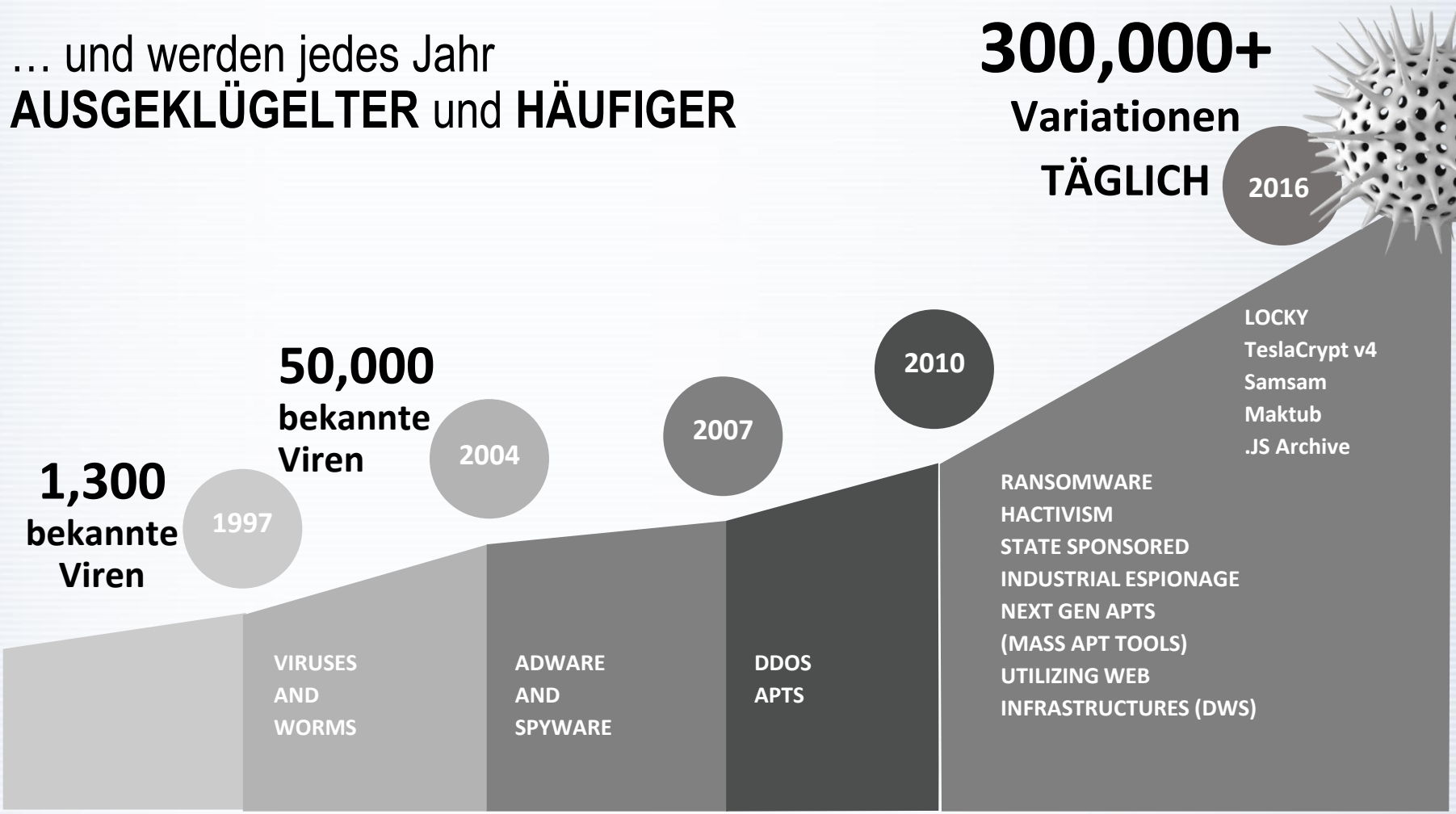
Talos, eine Abteilung von Cisco, konnte das Angler Exploit Kit im Juli bei der Arbeit beobachten. Anschließend wurden zahlreiche Angler-Server offline genommen. Das dürfte die Einnahmen der Mafiabande um einige Millionen reduzieren, denn Angler

Die Erklärung ist einfach: „Weil es Geld bringt“

Die Gefahren und Angriffe steigen täglich...

… und werden jedes Jahr
AUSGEKLÜGELTER und **HÄUFIGER**

300,000+
Variationen
TÄGLICH

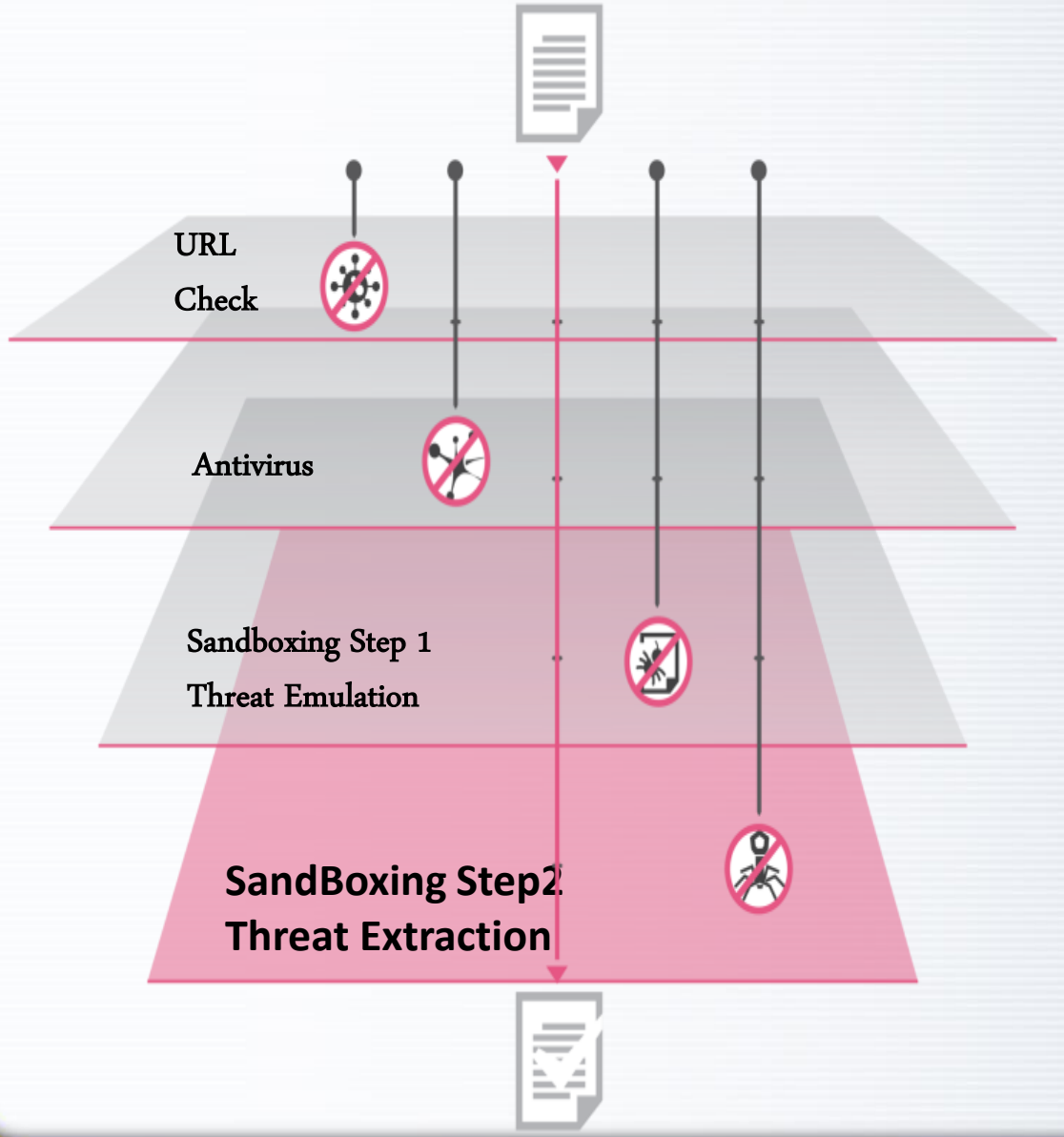


Reicht ein Virenscanner?

Heutzutage gibt es pro Tag über 300.000 neue Viren- und Schadprogrammvarianten. Klassische Anti-Virussoftware kann nicht mehr schnell genug aktualisiert werden.

Was ist zu tun?

Mehrstufiger Schutz!



Klassische Sandboxverfahren sind auch gefährdet!

Angreifer entwickeln kontinuierlich neue Umgehungs-Techniken:

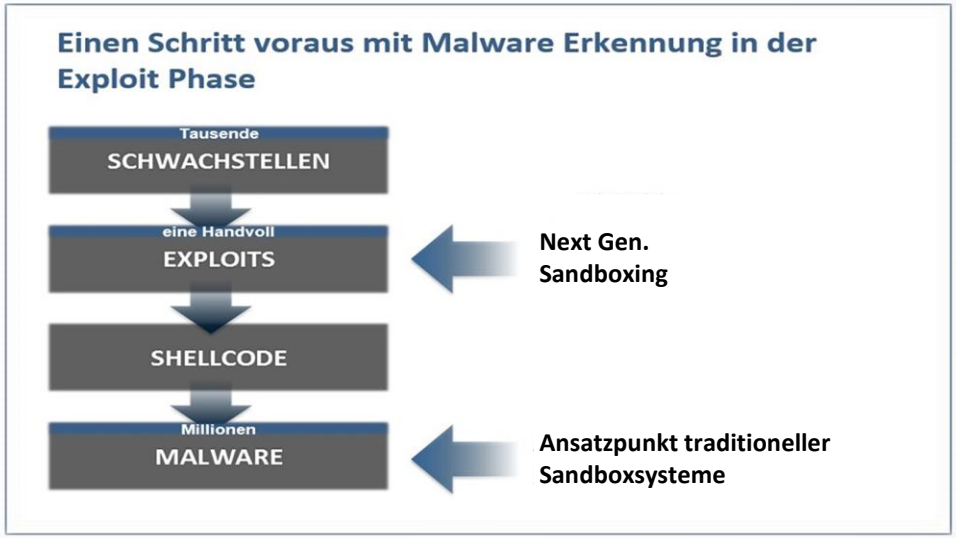
- Schadsoftware überprüft die Umgebung auf Sandboxmerkmale
- Schadsoftware setzt für eine bestimmte Zeit aus
- Schadsoftware wartet auf menschliche Interaktion
- ... “Katz und Maus” ...

Next Generation Sandboxing Step 1

Neue Sandbox-Lösungen bieten ein komplett neues und patentiertes Verfahren auf CPU-Ebene an.

Auf CPU-Ebene kann sich Schadsoftware noch nicht vor Sandboxen tarnen.

So entsteht eine extrem hohe Erkennungsrate.

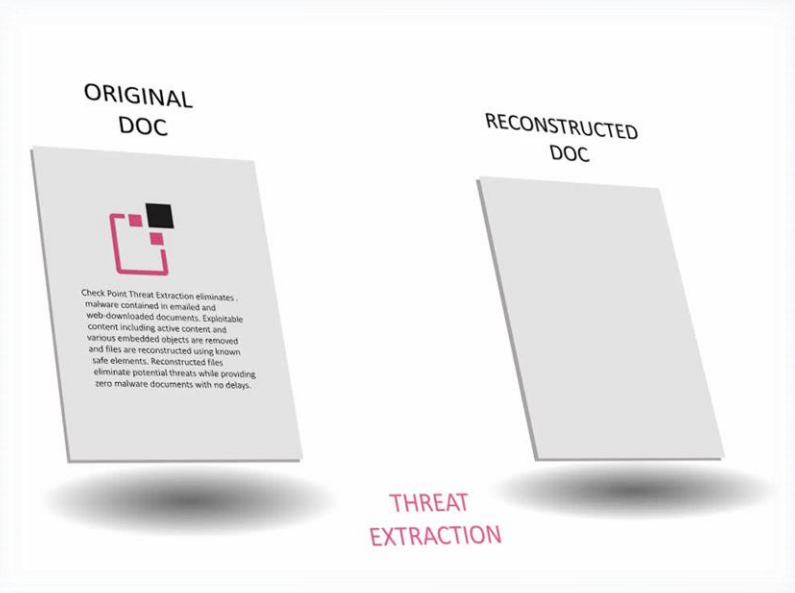


Next Generation Sandboxing Step 2

Aktive Inhalte bergen in Dokumenten immer potentielle Gefahren für den Anwender, weil sie Schadcode enthalten können.

Sehr wenige Anwender benötigen jedoch diese aktiven Inhalte.

Eine „Threat Extraction“ kann sichere Dokumente erzeugen.



Ein Beispiel anhand eines NetUSE-Kunden

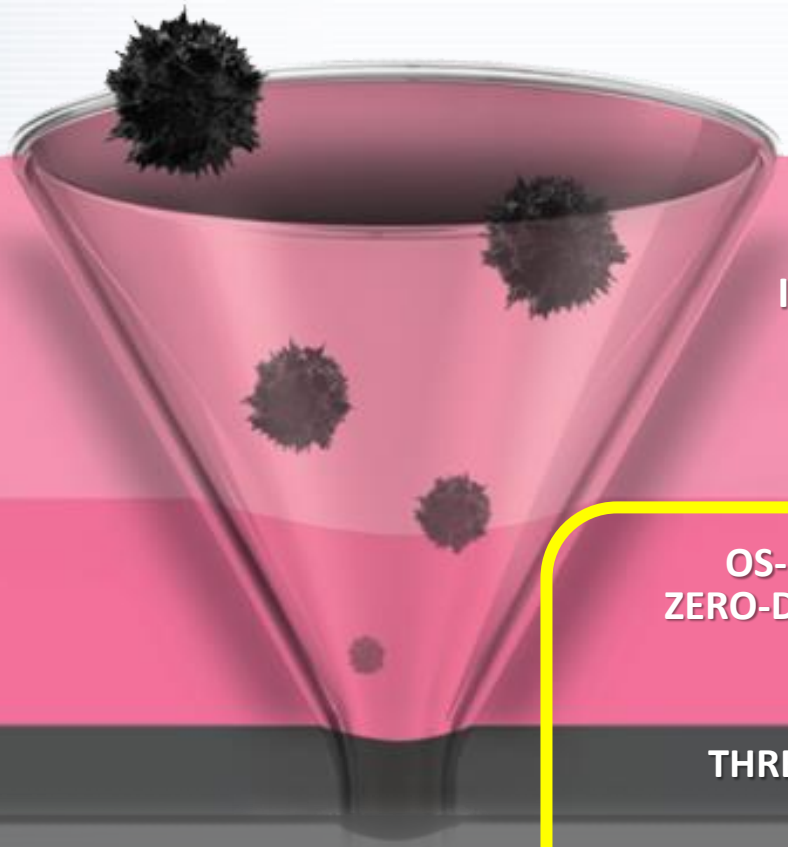
NetUSE-Kunden setzen Next Gen. Sandboxen schon sehr erfolgreich ein.
Es werden unbekannte Bedrohungen erkannt, die ohne diese Technik ungehindert bis zum Endanwender durchgedrungen wären.

Statistik eines durchschnittlichen Monats:

- Nach Anti-Spam zugestellte E-Mails: 114.670
- Funde der Standard Anti-Virus Lösung: 7
- Zusätzlich durch die Sandbox emulierte Dateien: 7.448
- Durch die Sandbox gefundene unbekannte Malware: 59

Es wurden somit 59 mögliche Infektionen rausgefiltert, die ohne die Lösung direkt in das Firmennetzwerk eingedrungen wären.

Zusammenfassung:



IPS, ANTI-VIRUS & ANTI-BOT

SCHÜTZT VOR BEKANNTER UND ALTER MALWARE

OS- UND CPU-LEVEL ZERO-DAY PROTECTION

SCHÜTZT VOR UNBEKANNTER UND NEUER MALWARE

mit OS- und CPU-level Schutz

THREAT EXTRACTION

VOLLSTÄNDIGE ENTFERNUNG VON ALLEN GEFAHREN

das Dokument wird in ECHTZEIT rekonstruiert und malwareFREI ausgeliefert

Vielen Dank für Ihre Aufmerksamkeit!

Björn Kirchberg
Produktmanager Security

NetUSE AG
Dr.-Hell-Straße, 24107 Kiel
Fon +49 (0)431 23 90 400
Fax +49 (0)431 23 90 499
info@NetUSE.de
http://www.NetUSE.de