



Gefahrenabwehr in der Praxis

Yvonne Bernard





HORNETSECURITY®

Überblick

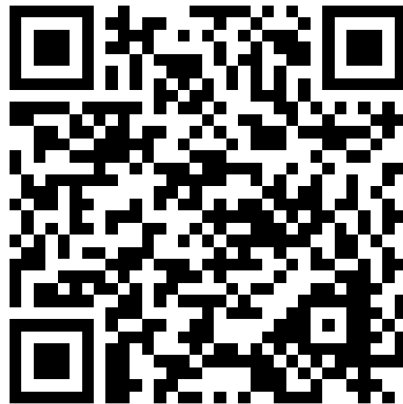
- Über Hornetsecurity und mich
- Motivation
- Angriffsarten
- Gefahrenabwehr
 - Sandboxanalyse Ransomware
 - ATP Engines bei Testkunden
- Fazit



HORNETSECURITY®

Über Hornetsecurity und mich

> Yvonne Bernard





HORNETSECURITY®

Motivation

CEO-FRAUD

Autozulieferer Leoni um 40 Millionen Euro betrogen

Mit dem sogenannten Chef-Trick erbeuten Kriminelle oft Millionenbeträge von Unternehmen. Mit fingierten [E-Mails](#) und Zahlungsanweisungen werden illegale Geldtransfers eingeleitet. Jetzt hat es einen großen deutschen Automobilzulieferer getroffen.

Der deutsche Automobilzulieferer Leoni ist um rund 40 Millionen Euro betrogen worden, [wie das Unternehmen am Dienstag selbst bekanntgegeben hat](#) [↗](#). Die Angreifer nutzten dabei offenbar eine als Chef-Trick oder CEO-Fraud bekannt gewordene Masche, um sich Zugriff auf die Zahlungen zu sichern.

Quelle: <http://golem.de>, 17.8.2016, 11:19



HORNETSECURITY®

Angriffsarten

Targeted Attacks

CEO-Fraud, Spearphishing und Whaling sind auf herkömmlichem Wege kaum zu erkennen. Hornetsecurity ATP unterbindet diese Angriffe konsequent. (z.B. Feign Facts Identification, IRS,...)

Ransomware

Erkennungsmechanismen wie die **Sandbox**-Engine und das **Freezing** enttarnen Locky, Tesla und andere polymorphe Viren.

Digitale Spionage

Das **Spy-Out Forensiksystem** erkennt bekannte und unbekannte Signaturen und schützt Unternehmen, bevor sensible Informationen nach außen dringen.



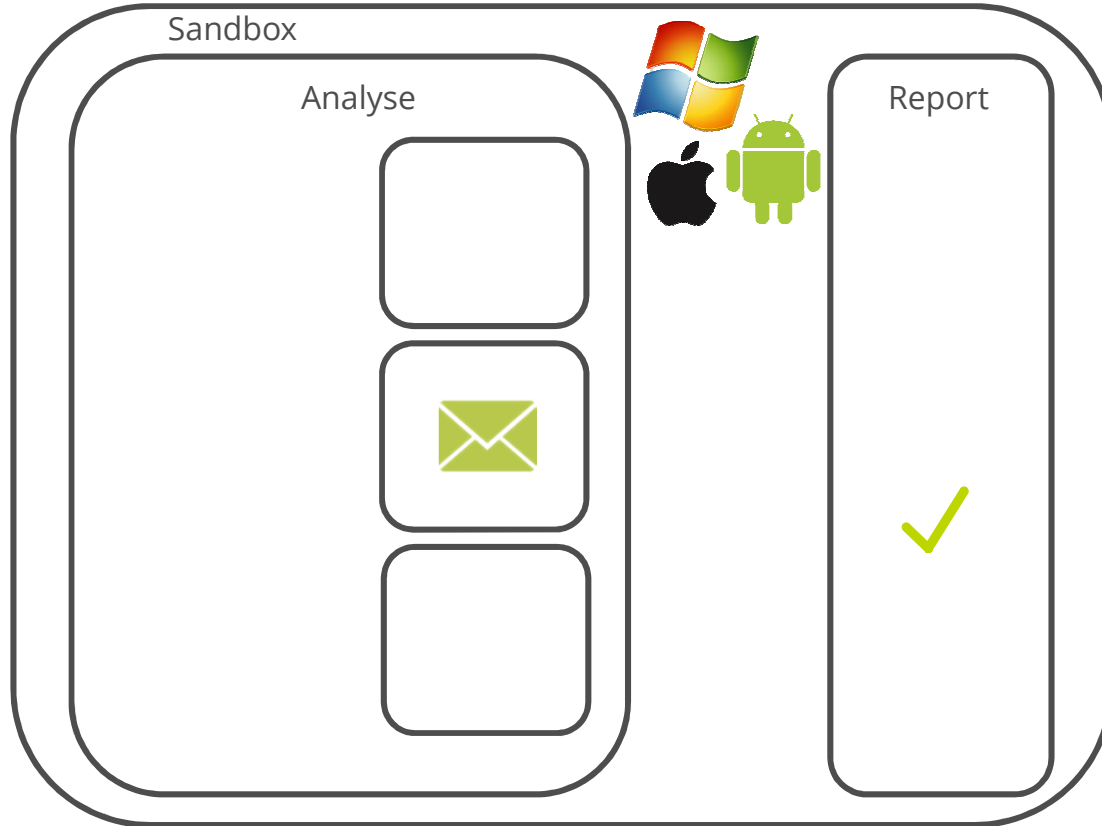
Blended Attacks

„Gemischte“ Angriffe (E-Mails mit Link auf Downloadseite im Anhang) sind schwierig abzuwehren. Mit verschiedenen Engines schafft Hornetsecurity ATP die nötige Sicherheit. (z.B. **URL Rewriting**, **URL Scanning**)



HORNETSECURITY®

Sandbox Engine (1/2)

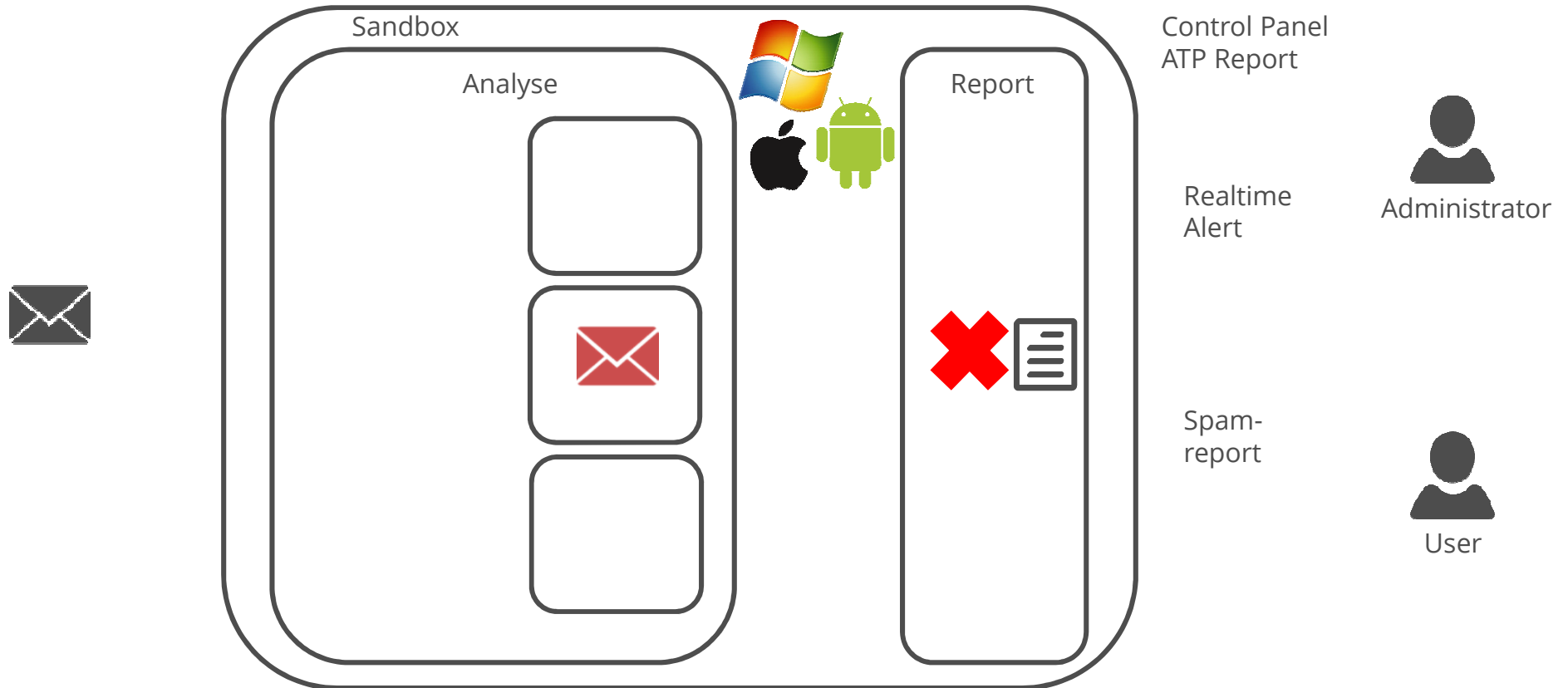


User



HORNETSECURITY®

Sandbox Engine (2/2)





HORNETSECURITY®

Bsp. Ransomware in der Sandbox

[Hitler Ransomware Hornetsecurity ATP.htm](#)


[Zeus.htm](#)



HORNETSECURITY®

Live Demo Hitler-Ransomware

This is the Hitler-Ransomware



Your Files was encrypted!

Do you decrypt your Files?
Buy a Vodafone Card (25€) and add the code
in the TextBox!

Cash Code(25€):

Your Files delete in: Decrypt

0 minutes 1 hour



HORNETSECURITY®

Live-Demo Zeus

Von Jeannine Mercado <Mercado.47581@...>
 Betreff **Confirmation letter**
 An [redacted]

Dear customer,
 The bank has sent loan confirmation letter. Please review the amount of funds.
 Many thanks,
 Jeannine Mercado
 Personal Manager

1 Anhang: 1148d0e3b8.zip

1148d0e3b8.zip\
 Datei Bearbeiten Ansicht Favoriten Extras Hilfe
 Hinzufügen Entpacken Überprüfen Kopieren Verschieben Löschen
 Name
 2f81882113c6a9d3133b427d3cb60adb1bc9d6c4e8277a8512cb6c35a7e83276.exe
 1 Objekt(e) markiert 634 032 634 032 2016-09-03 14:18

Hornetsecurity Pattern Analysis

- Presents an Authenticode digital signature
- Creates RWX memory
- Mimics the system's user agent string for its own requests
- At least one IP Address, Domain, or File Name was found in a crypto call
- Starts servers listening on 127.0.0.1:11684, 0.0.0.0:34799, :0
- Reads data out of its own binary image
- File has been identified by at least one AV-Engine as malicious
- Drops a binary and executes it
- Executed a process and injected code into it, probably while unpacking
- Code injection with CreateRemoteThread in a remote process
- Tries to unhook or modify Windows functions monitored by the sandbox agent
- Installs itself for autorun at Windows startup
- Creates Zeus (Banking Trojan) mutexes
- Zeus P2P (Banking Trojan)
- Creates a copy of itself
- Creates a slightly modified copy of itself
- Collects information to fingerprint the system

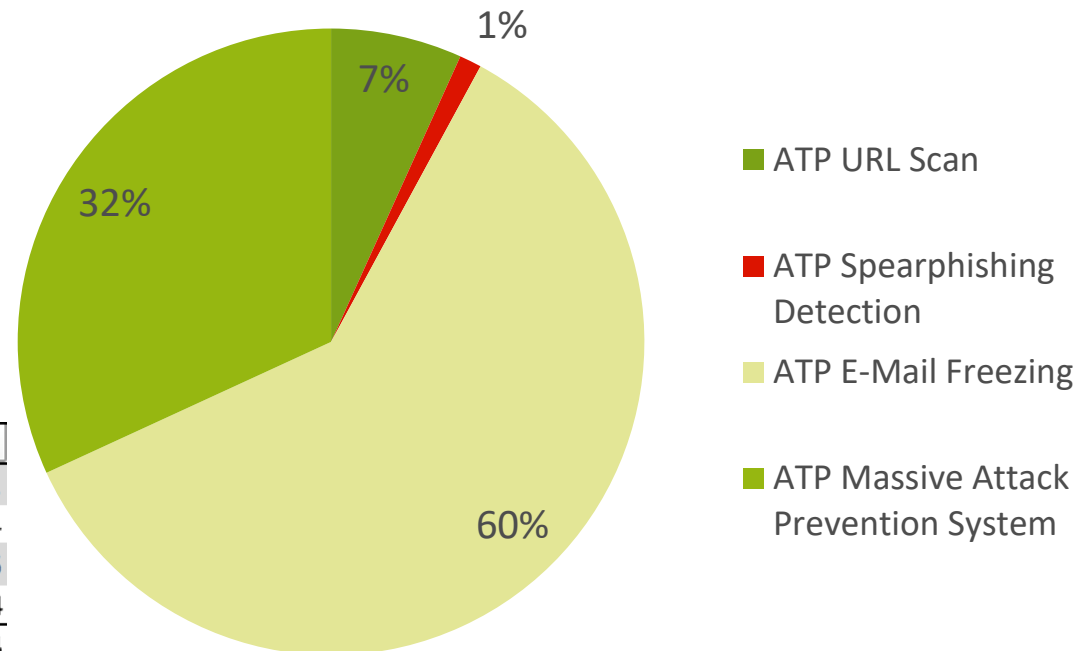


HORNETSECURITY®

ATP Engines bei Testkunden (1/2)

> August 2016

Verteilung der abgewehrten Angriffe auf ATP Engines



Grund	Anzahl
ATP URL Scan	141
ATP Spearphishing Detection	24
ATP E-Mail Freezing	1255
ATP Massive Attack Prevention System	664
Ergebnis	2084

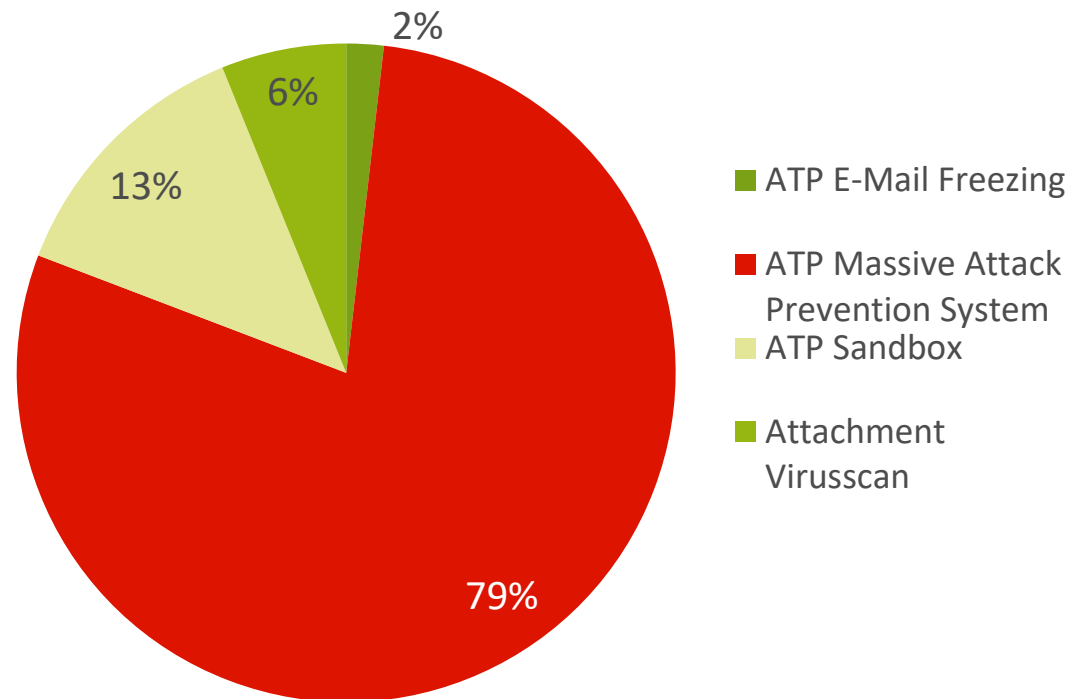


HORNETSECURITY®

ATP Engines bei Testkunden (2/2)

> August 2016

Filtererfolg nach Freezing und Rescan



Grund nach ATP E-Mail Freezing	Anzahl
ATP URL Scan	0
ATP Spearphishing Detection	0
ATP E-Mail Freezing	23
ATP Massive Attack Prevention System	991
ATP Sandbox	164
Attachment Virusscan	77
Ergebnis	1255



HORNETSECURITY®

Fazit

- Verschiedene Angriffsarten erfordern verschiedene Gegenmaßnahmen
 - Transparente Analyse von Ransomware in Sandbox
 - Angriffe werden immer intelligenter
 - Diverse weitere erfolgreiche weitere Engines im Hintergrund
- Eine Sandbox alleine hätte die 40 Mio.€ der Leoni nicht retten können



HORNETSECURITY®

Fragen?



<https://www.hornetsecurity.com/de/services/schutz-vor-ransomware-advanced-threat-protection>