


INCIDENT RESPONSE READINESS

... UND WIENER SCHNITZEL



Christian Wojner
(wojner@cert.at)

TLP:GREEN

PERSON	PUBLIKATIONEN	VORTRAGENDER
<p>Christian Wojner</p> <ul style="list-style-type: none">- Malware Analyse- Reverse Engineering- IT Forensik- Incident Response- Tool Development <p>Senior Malware & IT Forensics Analyst @ CERT.at, GovCERT Austria, AEC</p>	<p>Papers</p> <ul style="list-style-type: none">- Mass Malware Analysis: A DIY Kit- An Analysis of the Skype IMBot Logic and Functionality- The WOW-Effect <p>Articles</p> <ul style="list-style-type: none">- HITB Online Mag<ul style="list-style-type: none">- <i>The Art of DLL Injection</i>- <i>Automated Malware Analysis - An Intro to Minibis</i>- HAKIN9 Online Mag<ul style="list-style-type: none">- <i>Minibis</i> <p>Software</p> <ul style="list-style-type: none">- Minibis- Bytehist (REMnux, SIFT Workstation, SANS Trainings)- Densityscout (REMnux, SIFT Workstation, SANS Trainings)- ProcDOT (REMnux, SANS Trainings)	<ul style="list-style-type: none">FIRST Symposium 2010CertVerbund-DE 2010DeepSec 2010Teliasonera 2011Joint FIRST/TF-CSIRT Technical Seminar 2012CanSecWest 2012CertVerbund-DE 2012Oct0b3rf3st 2012SANS Forensics Prague 2012DeepSec 2012FIRST Symposium 2013CertVerbund-DE 2013Oct0b3rf3st 2013SANS Forensics Prague 2013CENTR Meeting 2013ATC Jahrestreffen 2014Oct0b3rf3st 2014IT-SeCX 2014DeepSec 2014DeepIntel 2017Jahresforum SecurITy 2017ATC Jahrestreffen 2021ATC Jahrestreffen 2022IMH Forum IT 2022IMH Forum IT 2023 <p>+ Closed Conferences + Trainer/Instructor</p>
	<p>ZERTIFIZIERUNGEN</p> <ul style="list-style-type: none">- Malware Analyse/Reverse Engineering: GREM, CREA, CERA- Digital/Computer Forensik: GCFA	

Unsere Verteidigung ist gut, aber ...

- Angreifer brauchen nur EINE Lücke ...
- Angreifer brauchen nur EINMAL Erfolg ...
- Wir müss(t)en IMMER erfolgreich sein ...
- Wir sind aber auch von anderen abhängig ...
- Es ist also nur eine Frage der Zeit ...



... daher ...

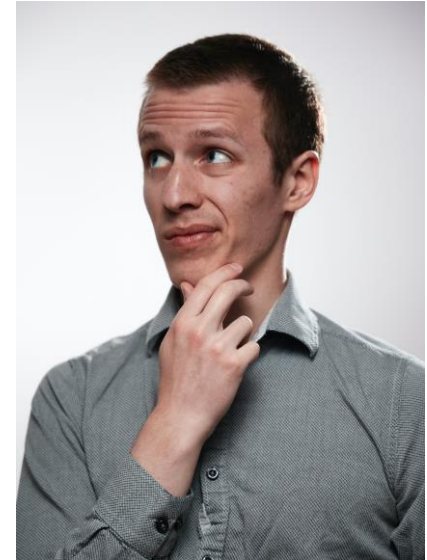
- Angreifer brauchen nur EINE Lücke ...
- Angreifer brauchen nur EINMAL Erfolg ...
- Wir müss(t)en IMMER erfolgreich sein ...
- Wir sind aber auch von anderen abhängig ...
- Es ist also nur eine Frage der Zeit ...



**... Erwarte die
KOMPROMITTIERUNG!**

Begriffsdefinitionen

- Incident
 - IT Security relevanter Vorfall
- Incident Response
 - Reaktion auf einen/Behandlung eines Incident/s
- Incident Response Plan
 - Angestrebte Vorgehensweise bei Incident Response
- **Incident Response Readiness**
 - **Vorbereitung/Einsatzbereitschaft auf/für Incident Response**



Incident Response Readiness (IRR)

- Hat Ihr Unternehmen schon etwas für IRR gemacht?
- IRR macht IR
 - überhaupt erst möglich
 - deutlich effizienter
 - qualitativ hochwertiger
 - günstiger
 - entspannter
- Sehen Sie IRR als Ihre persönliche Chance!



IRR ist ein Gesamtpaket!

Ausrüstung



Ressourcen

Planung



Ausbildung



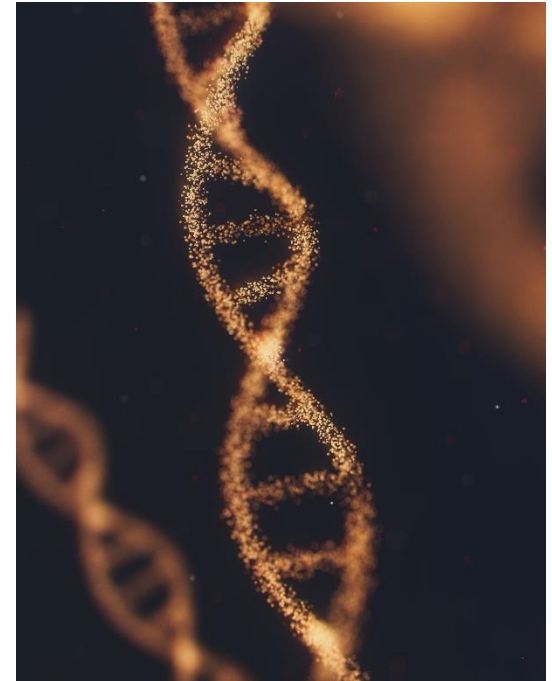
Datensammlung



Training

IR Datenbasis

- Grundlage von IR sind immer Daten!
- Ohne Berücksichtigung im Vorfeld, sind viele davon im Notfall aber nicht verfügbar!
- Log-orientierte Daten (Logs)
- Daten(-mitschnitte)
- Vergleichsdaten
- Daten-Sicherungen
- Sonstiges



IR Datenbasis: Log-orientiert

- DNS Logs
- Firewall Logs
- Proxy Logs (Proxy-Zwang?!)
- DHCP Logs
- Windows Event Logs
 - Audit Optionen aktivieren! (Advanced Audit Policy Settings, Powershell, ...)
 - Sysmon (Commandline/Process Logging)
- Linux Syslog
- ...
- It'a matter of time ... Zeit-Synchronisation und Zeit-Zonen
- Wichtig: Zentrales Logging!
 - Selten aber doch: Virtualisierte Clients
- Log Retention Time → So lange wie möglich!

IR Datenbasis: Log-orientiert

- DNS Logs
- Firewall Logs
- Proxy Logs (Proxy-Zwang?!)
- DHCP Logs
- Windows Event Logs
 - Audit Optionen aktivieren! (Advanced Audit Policy Settings, Powershell, ...)
 - Sysmon (Commandline/Process Logging)
- Linux Syslog
- ...
- It'a matter of time ... Zeit-Synchronisation und Zeit-Zonen
- Wichtig: Zentrales Logging!
 - Selten aber doch: Virtualisierte Clients
- **Log Retention Time → So lange wie möglich!**

Ein bekanntes deutsches Technologieunternehmen:

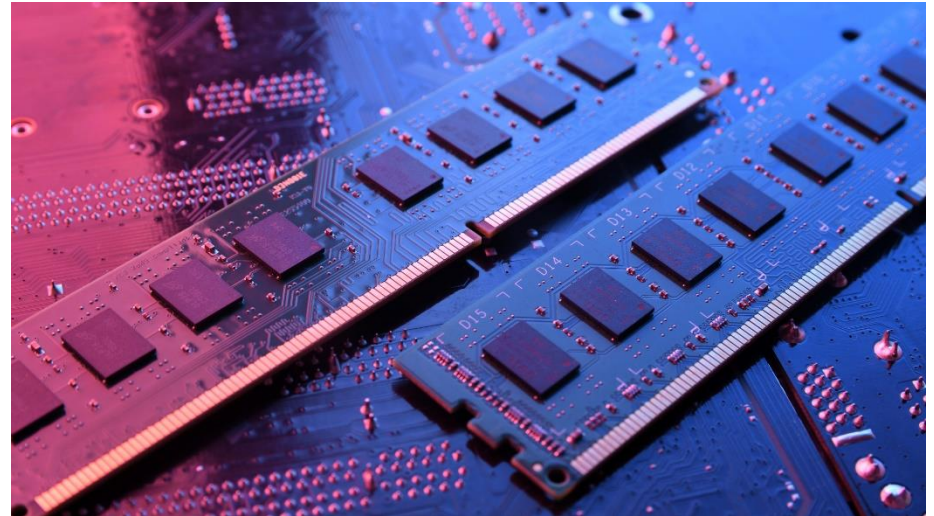
"Besucher" zufällig entdeckt, bereits 1,5 Jahre unterwandert

Turla und der Deutsche Bundestag:

"Ende 2016 drangen russische Hacker in das Datennetzwerk des Bundes ein ... im Dezember 2017 entdeckte das Bundesamt für Sicherheit in der Informationstechnik den Angriff" (*Wikipedia*)

IR Datenbasis: Daten(-mitschnitte)

- Prefetch
 - Wichtig: (Auch) auf Servern aufdrehen!
- Memory Dump
 - FTK Imager
 - winpmem („_mini“-Version wegen RAW Format!)
- Netflows
- PCAPs
 - Mirror Ports
 - TLS aufbrechen!



IR Datenbasis: Vergleichsdaten

Deutliche Effizienzsteigerung bei der Suche nach Spuren, Verdächtigem und effektiver Schadsoftware

- Baselines → Was ist in meinem Netz/auf meinen Rechnern normal?
 - Persistenzen
 - Prozesse
 - Connections
 - Installierte Software
 - Files
 - Registry
- Golden Images → Basis-Setup für Clients (manchmal auch Server)
- Volume Shadow Copies
- Backups
- VM Snapshots



IR Datenbasis: Daten-Sicherungen

- Unverzichtbar für die Wiederherstellung!
 - Manchmal letztes Ass im Ärmel, um doch noch Spuren zu finden!
-
- Volume Shadow Copies
 - Backups (+ offline!)
 - VM Snapshots (+ offline!)



IR Datenbasis: Sonstiges

Nicht unbedingt per se „Daten“, aber Dinge, die mit der IR Datenbasis, bzw. mit deren Sammlung, zu tun haben.

- CMDB (Configuration Management Database) / Asset DB
 - Finde den/die betreffenden Rechner/Komponenten
- Netzwerkplan
- Fulldisk Encryption Keys
- IP Adressen Pseudonymisierung (Umkehrung!)
- Admin-Rechte werden benötigt werden



IR (Collection) Agents & Co

- Im Fall des Falles sehr hilfreich
- Müssen nicht mehr nachträglich installiert werden
 - Alarmiert den Angreifer nicht
 - Keine Ausrollprobleme
- Beispiele (gratis)
 - Kape
 - Velociraptor



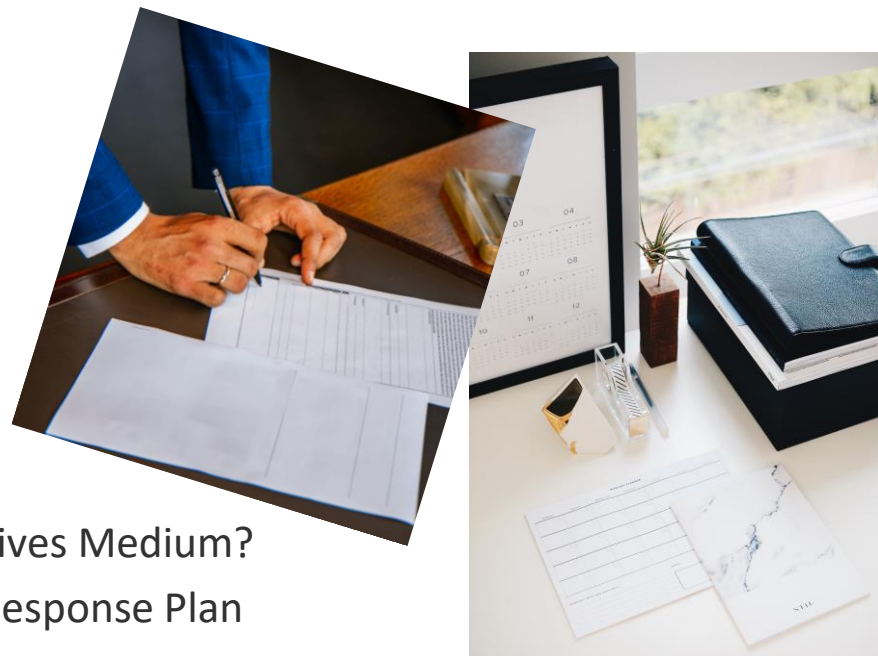
IR Dienstleister

- Gibt's schon einen Vertrag?
- Know your Gegenüber!
- Frage IR Dienstleister nach seinen IRR Erwartungen
 - Log Retention Times
 - Log Config
 - ...
- IR (Collection) Agents & Co?
 - Gibt es bereits ausgerolltes?
 - Sollte es sowas geben?



IR non-geeky Stuff

- Kontaktliste aller IR Player
- Presseaussendungen
- Cyber Versicherung
- Meldungen
 - Polizeiliche Anzeige
 - NIS
 - DSGVO
 - Cyber Versicherung
 - Aktionäre
 - ...
- Unternehmensspezifisches?
- Kommunikation im Ernstfall → Alternatives Medium?
- Zusammenspiel der Kräfte → Incident Response Plan



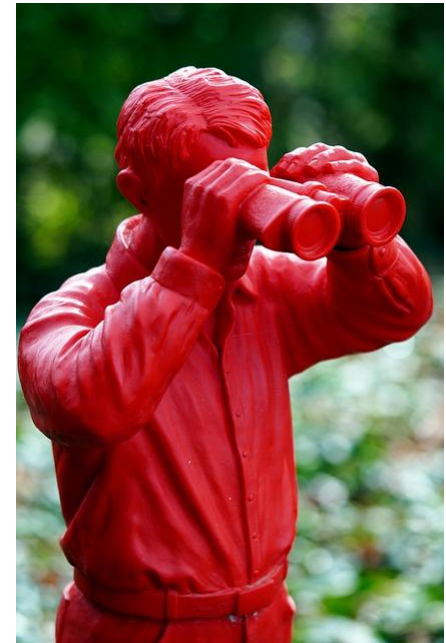
Der Drucker als IRR Player

- Drucke Wichtige Dokumente aus ... solange es noch geht!



Detection is Key!

- Danach kommt's auf Retention Time an
- Tools (IDS, EDR, AV, ...)
- Bei APT's: Hinweis auch oft durch Dritte
- Verhalten der Mitarbeiter schulen
 - User → Meldungen machen + keine Angst davor
 -
 -
 -
 - Admins → Richtige (erste) Reaktion ...



Erste Reaktion

- Hat enormes Beeinflussungspotential auf das IR Ergebnis!
- Unsicher? → Überleg lieber einmal mehr!
- Handle nie unüberlegt!
- Lass Dir Zeit und mach alles so richtig wie möglich!
- **Falsch!**
 - Betroffenen Rechner runterfahren
 - Enterprise/Domain Admin verwenden
- **Richtig!**
 1. Mache Memory Dump (wenn sinnvoll)
 2. Strom weg!
 - Isolieren ist aber auch eine Option
 - LAPS, Wegwerf-Admin, ...
- Merke: Definiere diesen Prozess unbedingt im **Vorfeld** (IRR!) und **übe** es **periodisch**!



IRR Wirksamkeit/Bewertung

- Funktionieren alle gesetzten Schritte?
 - Reichen die Daten/Logs/Tools?
 - Ziehen alle an einem gemeinsamen Strang?
 - Werden wir im Ernstfall bestehen?
 - Wo können wir etwas besser machen?
 - Haben wir einen blinden Fleck?
- ➔ Pen-Tests helfen hier nicht!
- ➔ Unser Ansatz: „IRR Schnitzeljagd“



„IRR Schnitzeljagd“

- Kein Pen-Test!
- Wir spielen live in Produktion!
- Nix kann kaputt werden!
- Echte Aussagekraft!
- Jedes Ergebnis ist wertvoll!
- Bestrafe nicht!
- Rollen
 - Externer „Hinweisgeber“ (CERT)
 - Eingeweihter „Komplize“ (CISO)
 - Uneingeweihte „Spieler“ (Mitarbeiter)



„IRR Schnitzeljagd“: Ablauf

1. Wir (CERT) haben mehrere spezielle Domains registriert
 - Die zeigen auf unterschiedliche IP Adressen wo jeweils ein Web Server läuft
2. „Komplize“ geht zu beliebigem Rechner und ruft eine URL (spezielle Domain!) auf
 - Response muss nicht unbedingt 200 sein!
3. Einen Monat warten (kann auch länger sein ... individuell anpassbar)
4. „Komplize“ macht einen weiteren Zugriff
 - auf dem ursprünglichen Rechner
 - oder einem anderen
 - auf die gleiche URL
 - eine andere URL auf der bereits besuchten Domain
 - oder sogar auf eine andere Domain
5. Schritte 2-3(4) sind beliebig wiederhol-/kombinierbar für unterschiedliche Szenarien/Aussagen
6. „Hinweisgeber“ schickt E-Mail mit beobachteten Zugriffen an das Unternehmen
7. IR Prozess („Spieler“!) nimmt Fahrt auf → Ergebnis
8. Client Aktivitäten/Forensik wäre/n grundsätzlich auch noch möglich



Reactions?

