



Professionelles Backdooring

Marc Ruef
www.scip.ch



ISMS
PRAXIS FORUM

ISMS Praxis Forum
04. September 2014, Olten

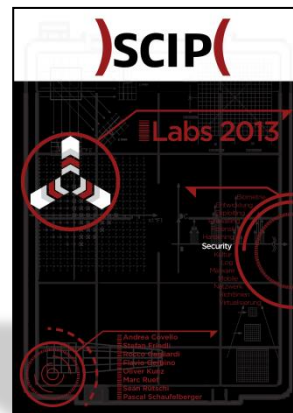
Agenda | Backdooring

1. Einführung	
Einführung	2 min
Wer bin ich?	1 min
Was ist das Ziel?	1 min
2. Vorbereitung	
Zieldefinition	3 min
Konzeptionierung	5 min
Entwicklung	5 min
Testing	5 min
3. Durchführung	
Infektion	3 min
Datensammlung	3 min
Exfiltration	3 min
4. Nachbearbeitung	
Desinfektion	1 min
Auswertung	5 min
Reporting	1 min
5. Abschluss	
Zusammenfassung	2 min
Fragen	5 min



Einführung | Wer bin ich?

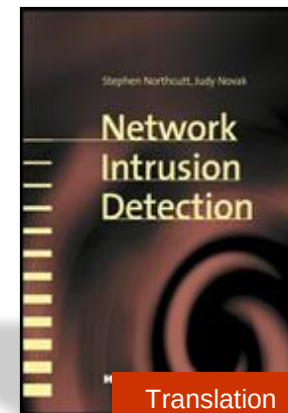
Name	Marc Ruef
Beruf	Mitinhaber / CTO, scip AG, Zürich
Private Webseite	http://www.computec.ch
Letztes eigenes Buch	„Die Kunst des Penetration Testing“, Computer & Literatur Böblingen, ISBN 3-936546-49-5



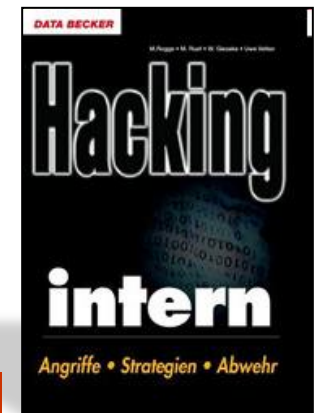
2013



2007



2004

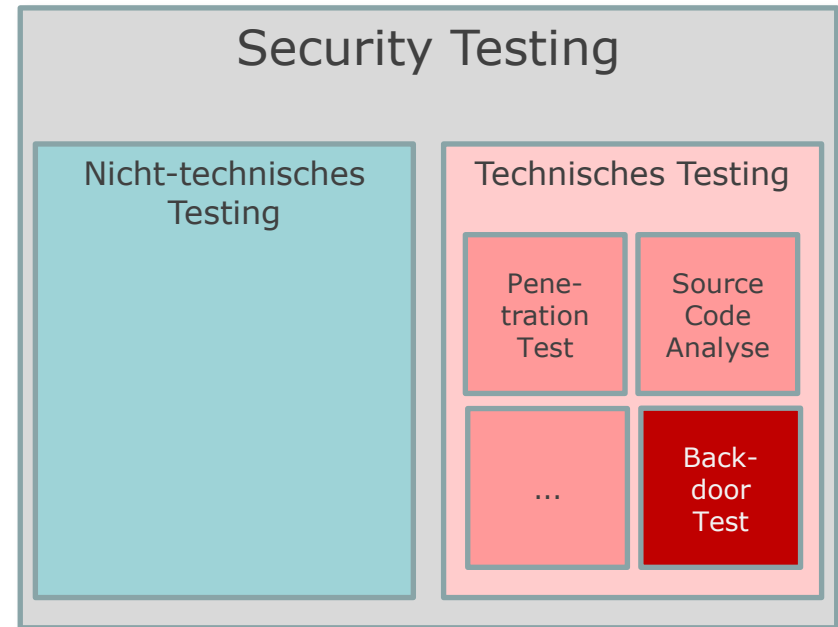


2002

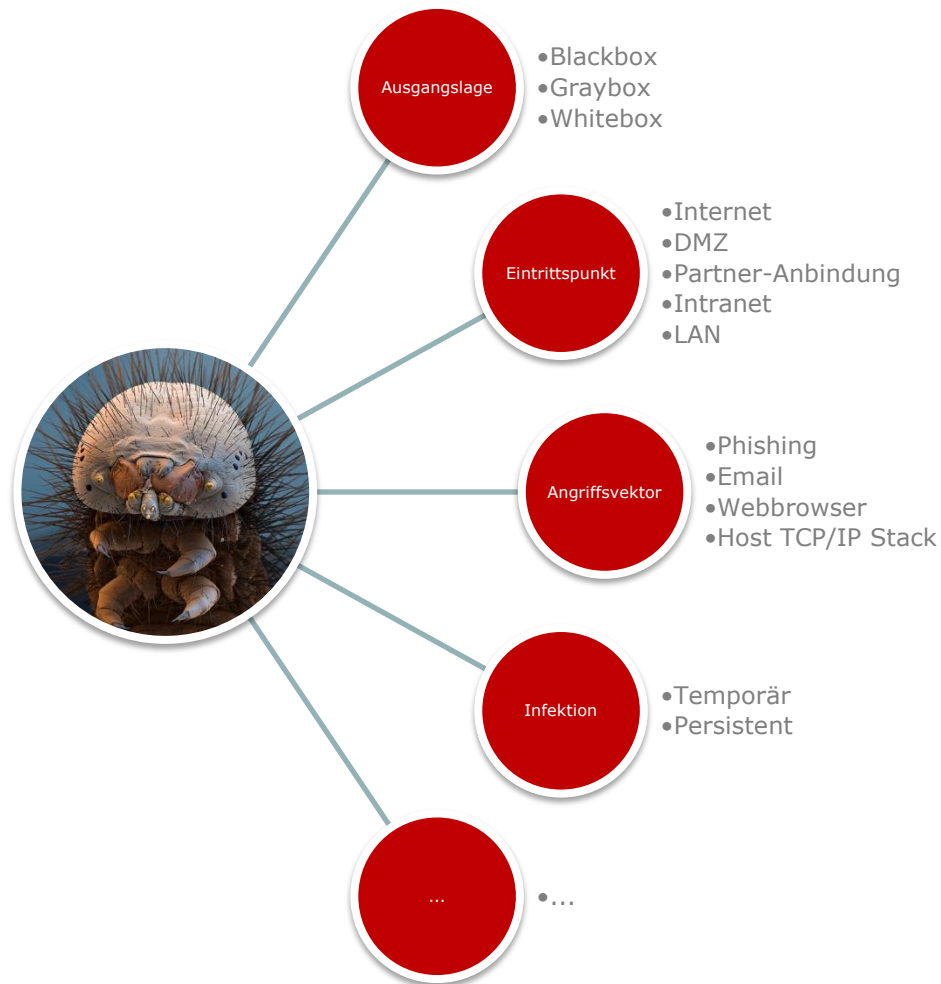


Einführung | Was ist das Ziel

- Sicherheitsüberprüfungen sollen Schwachstellen aufdecken
- Backdoor Tests sind eine spezielle Form von Prüfungen
- Durch kundenspezifische Malware werden sämtliche Facetten des Sicherheitsdispositivs geprüft:
 - Awareness
 - Mail / Web Client Sicherheit
 - Antiviren-Lösungen
 - Firewalling, IDS, IPS, DLP
 - Logging, Monitoring, Alerting, Incident Response



Vorbereitung | Zieldefinition



Vorbereitung | Konzeptionierung (Beispiel)

Aspekt	Definition	Beschreibung
Ausgangslage	Whitehat	Es stehen uns sämtliche Details zur Zielumgebung zur Verfügung
Eintrittspunkt	Internet	Extern
Angriffsvektor	Phishing + XSS	Es wird ein Phishing Email verschickt, das per Link auf die Firmenwebseite lockt. Dort wird durch eine bestehende XSS-Schwachstelle (in vorangegangenen Pentest gefunden) der Download eines SSL-Zertifikats vorgetäuscht.
Infektion	Temporär	Die Backdoor ist nur während der laufenden Sitzung aktiv. Spätestens ein Neustart deinstalliert sie.
Kommunikationskanal	HTTPS	Über einen API Call wird eine HTTPS-Verbindung aufgebaut. Anweisungen in der Queue werden über GET-Requests abgeholt und Resultate über POST-Requests hochgeladen.
Datensammlung	Host-Informationen, Screenshot	Es werden automatisch die über ipconfig.exe ausgegebenen Informationen als Proof-of-Concept übertragen. Zudem wird ein Screenshot erstellt, falls der SAP Client im Vollbildmodus und aktiv ist. Weitere Datensammlungen über Queue möglich.
Lebensdauer	≤31.12.2014	Das Projekt läuft bis am 24.12.2014, wobei am letzten Tag manuell per Queue ein unload() initiiert wird. Eine Ausführung nach dem 31.12.2014 ist nicht mehr möglich.



Vorbereitung | Entwicklung (AJAX Backdoor Beispiel)

```
1 var socket = 'socket.php';
2 var clientdebug = 0;
3 var xmlhttp = null;
4 var runnerinterval;
5 var interval = 5000;
6 var identifier;
7
8 function runner(){
9     runnerinterval = setInterval("send_request(socket + '?request=QUERY&identifier=' + identifier, receive_command)", interval);
10 }
11
12 function send_request(url, onreadystatechange){
13     xmlhttp = null;
14     if(window.XMLHttpRequest){
15         xmlhttp = new XMLHttpRequest();
16     }else if(window.ActiveXObject){
17         xmlhttp = new ActiveXObject('Microsoft.XMLHTTP');
18     }
19     if(xmlhttp != null){
20         xmlhttp.onreadystatechange=onreadystatechange;
21         xmlhttp.open('GET', url, true);
22         xmlhttp.setRequestHeader('If-Modified-Since', 'Fri, 31 Dec 1999 23:59:59 GMT');
23         xmlhttp.send(null);
24     }else{
25         clearInterval(runnerinterval);
26         alert('Your browser does not support XMLHttpRequest.');
```

Queue-Intervall 5 Sekunden

Runner fragt Queue ab

XMLHTTP als Mechanismus

Caching mit Header verhindern

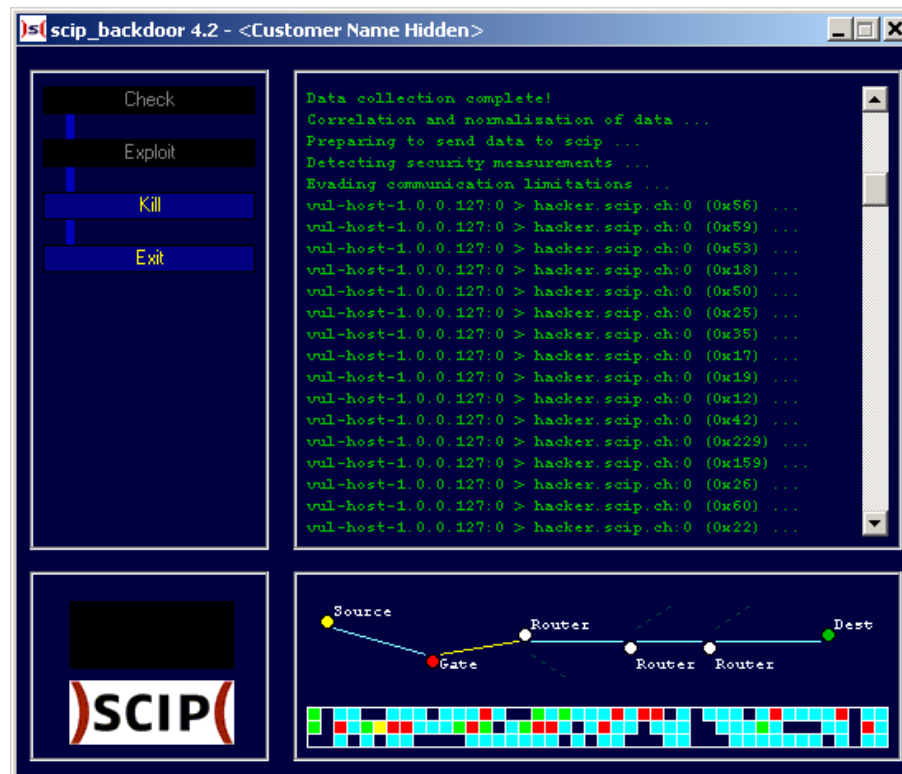
```
27     }
28 }
29
30 function receive_command(){
31     if(xmlhttp.readyState==4){
32         if(xmlhttp.status==200){
33             identifier = xmlhttp.responseXML.getElementsByTagName('identifier')[0].childNodes[0].nodeValue;
34             var response = xmlhttp.responseXML.getElementsByTagName('response')[0].childNodes[0].nodeValue;
35
36             if(clientdebug){
37                 var statuscode = xmlhttp.responseXML.getElementsByTagName('statuscode')[0].childNodes[0].nodeValue;
38                 var statustext = xmlhttp.responseXML.getElementsByTagName('statustext')[0].childNodes[0].nodeValue;
39                 var timestamp = xmlhttp.responseXML.getElementsByTagName('timestamp')[0].childNodes[0].nodeValue;
40                 var receiver = xmlhttp.responseXML.getElementsByTagName('receiver')[0].childNodes[0].nodeValue;
41                 show_debug('=> QUERY: ' + statuscode + ' (' + statustext + ') ' + timestamp + ' ' + identifier + ' ' + receiver + ' ' + response);
42             }
43         }
44     }
45 }
```

Elemente aus Response

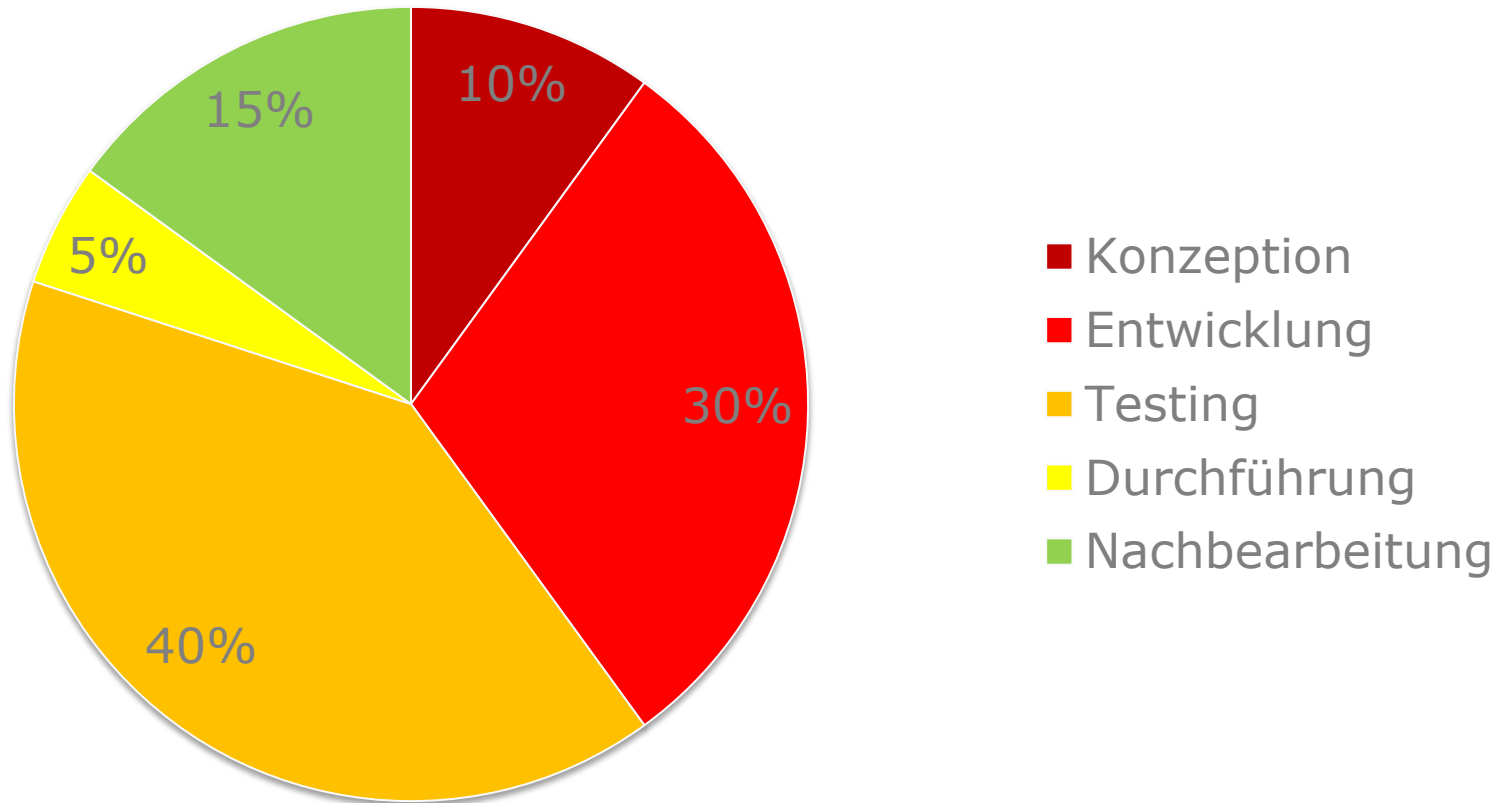
Debug View aktivieren



Vorbereitung | Entwicklung (VBA Backdoor Beispiel)



Vorbereitung | Aufwände im Vergleich



Vorbereitung | Testing Fokus

- Funktionalität
 - Infektion
 - Datensammlung
 - Kommunikation
 - Desinfektion
- Robustheit
 - Fallback-Szenarien (z.B. HTTPS → HTTP)
 - Fehler abfangen und unterdrücken
- Einschränkungen
 - Ablaufdatum
 - Binding an IP-Adressen, Hostnamen, Benutzernamen, ...





SCIP



5 x 2 Tickets mit Swiss ab
Zürich Kloten nach New York.
3 Übernachtungen im Hotel
Affinia in Manhattan.
CHF 1000.- Taschengeld

**4 TAGE SHOPPING
IN NEW YORK**

Helvetic Tours
Ein Wettbewerb von Helvetic Tours

Wichtig! Deklarations für spezielle Stichtagereisen: Angebote von Helvetic Tours zu erleben.
Möglicherweise kommen auch



Helvetic Tours Quiz

HelveticTours
We teure Ferien. Nur günstiger.

Welche Farbe haben Taxis in New York?

☐ Weiss
☐ Gelb
☐ Schwarz/Rot

Was ist das Wahrzeichen von New York?

☐ Big Ben
☐ Golden Gate Bridge
☐ Freiheitsstatue

Welcher berühmte Entertainer hat New York ein Lied gewidmet?

☐ Frank Sinatra
☐ Dean Martin
☐ Sammy Davis jr.

Zur Teilnahme am Wettbewerb ist jedermann zugelassen. Ausgenommen sind alle Mitarbeiter der Helvetic Tours und deren Familienangehörige. Die Gewinner werden schrittlich benachrichtigt. Die Preise können nicht bar ausbezahlt werden. Über den Wettbewerb wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Mitmachen & Gewinnen

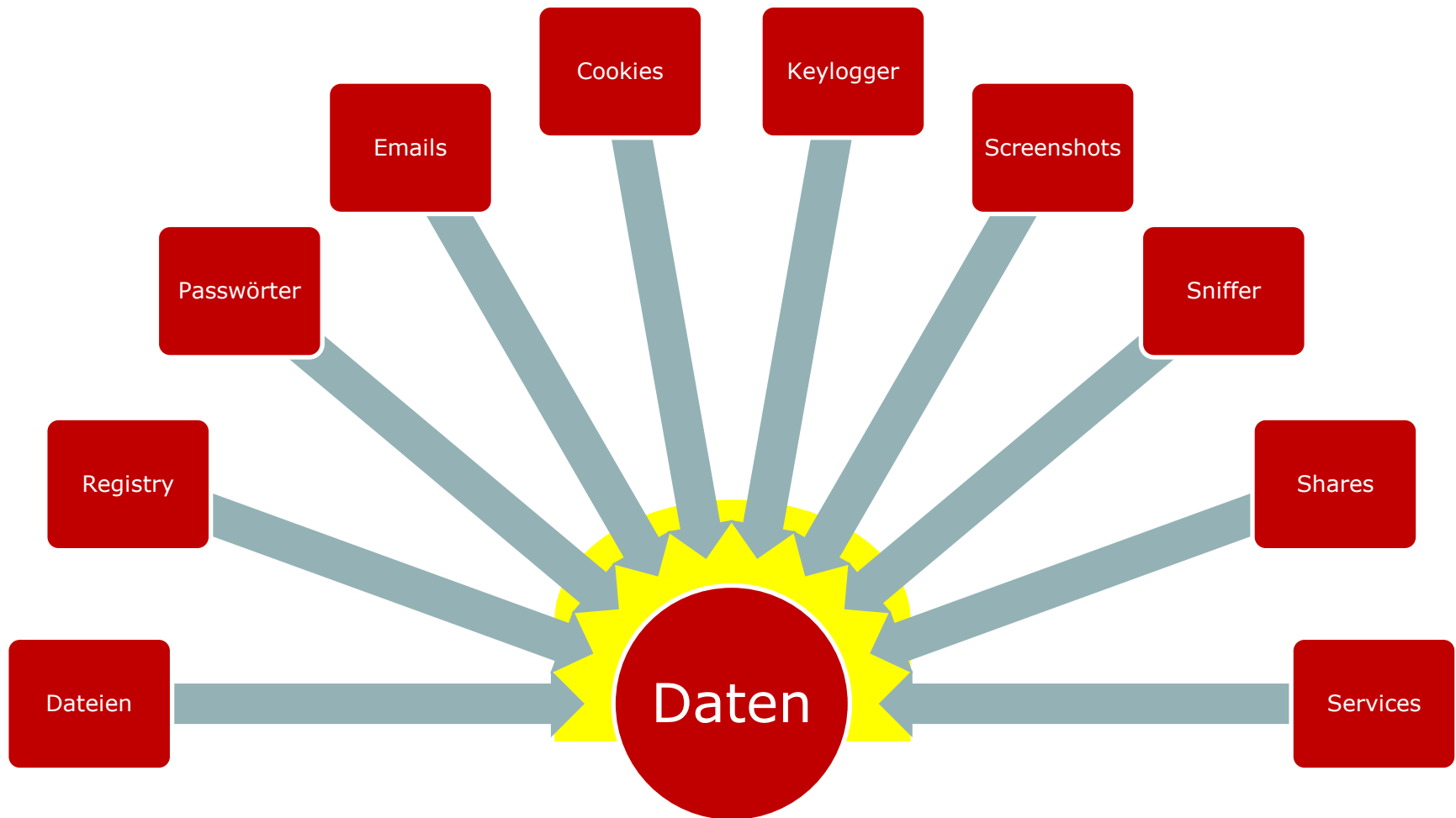


Durchführung | Infektion

- Zielpersonen + Zielsysteme müssen während des gesamten Tests identifizierbar sein



Durchführung | Datensammlung



Durchführung | Exfiltration

- Mindestens unidirektionale Verbindung erforderlich
- Bestehende Protokolle bieten sich an
 - HTTP, SMTP, FTP, NNTP, ...
- Komplexe Konstrukte unter Umständen erforderlich
 - Outlook ISAPI
- Entgehen der Entdeckung
 - API-Calls (z.B. ShellExecute() in Shell32.dll)
 - Tunneling (z.B. Kommandos in HTML über HTTP)
 - Encoding (siehe <http://www.computec.ch/projekte/spread/>)
 - Timing



Nachbearbeitung | Desinfektion

- Desinfektion wird initiiert
 - Verbundene Systeme erhalten unload() Anweisung
 - Timeout desinfiziert (relativ zum Test-Start bzw. Laufzeit)
 - Ablaufdatum desinfiziert und verhindert spätere Ausführung
- Desinfektion wird durchgeführt
 - Entfernen temporärer Dateien
 - Freigeben von Speicher
 - Entfernen der Binaries



Nachbearbeitung | Auswertung

- Infektionspfad muss pro Benutzer/System nachvollziehbar sein
 - Webbug in Email mit personalisierter URL
 - Download Link mit personalisierter URL
 - Backdoor liefert Username/Hostname/IP-Adresse
- Personenbezogene Informationen werden nicht an den Kunden weitergegeben

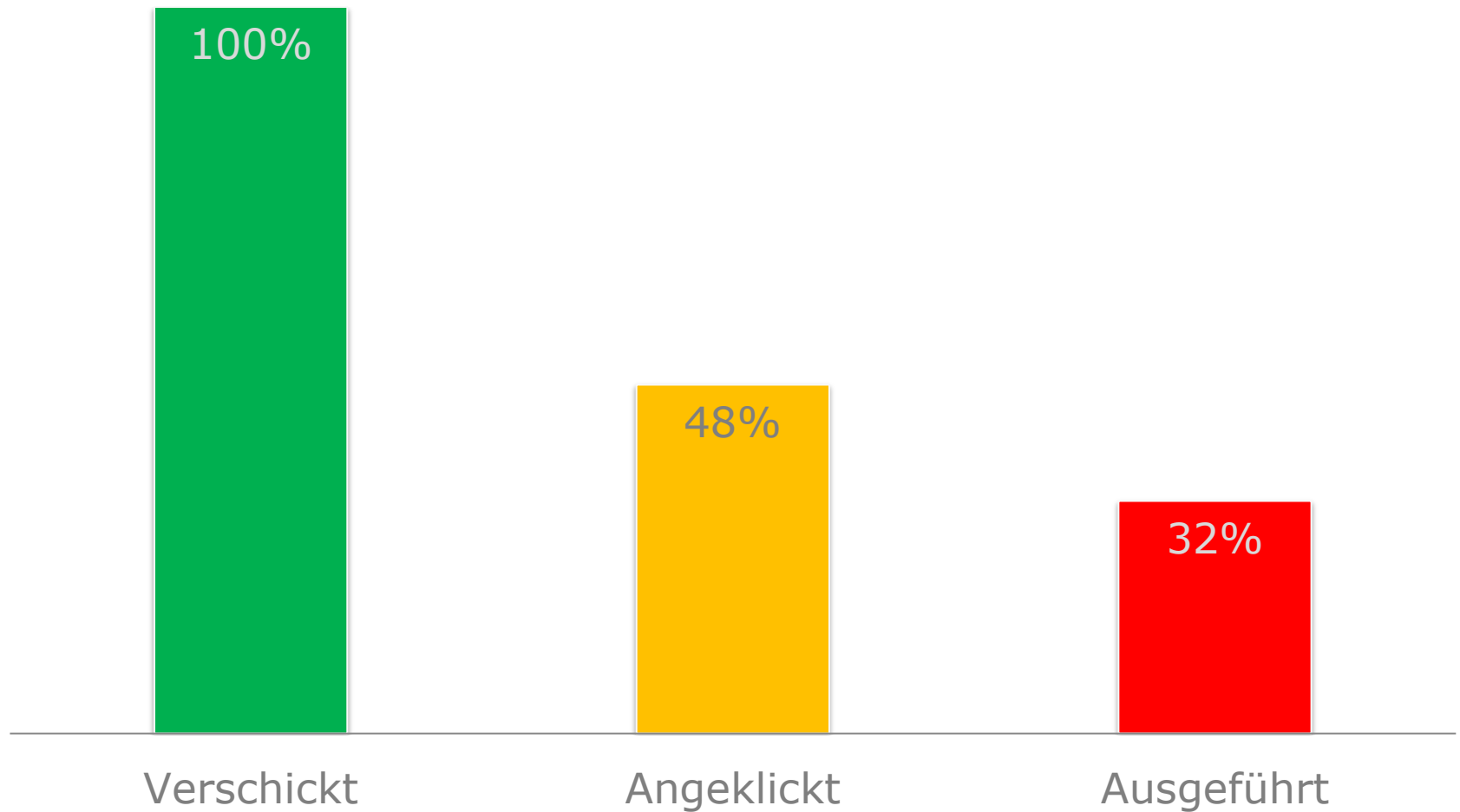


Nachbearbeitung | Auswertung (Beispiel)

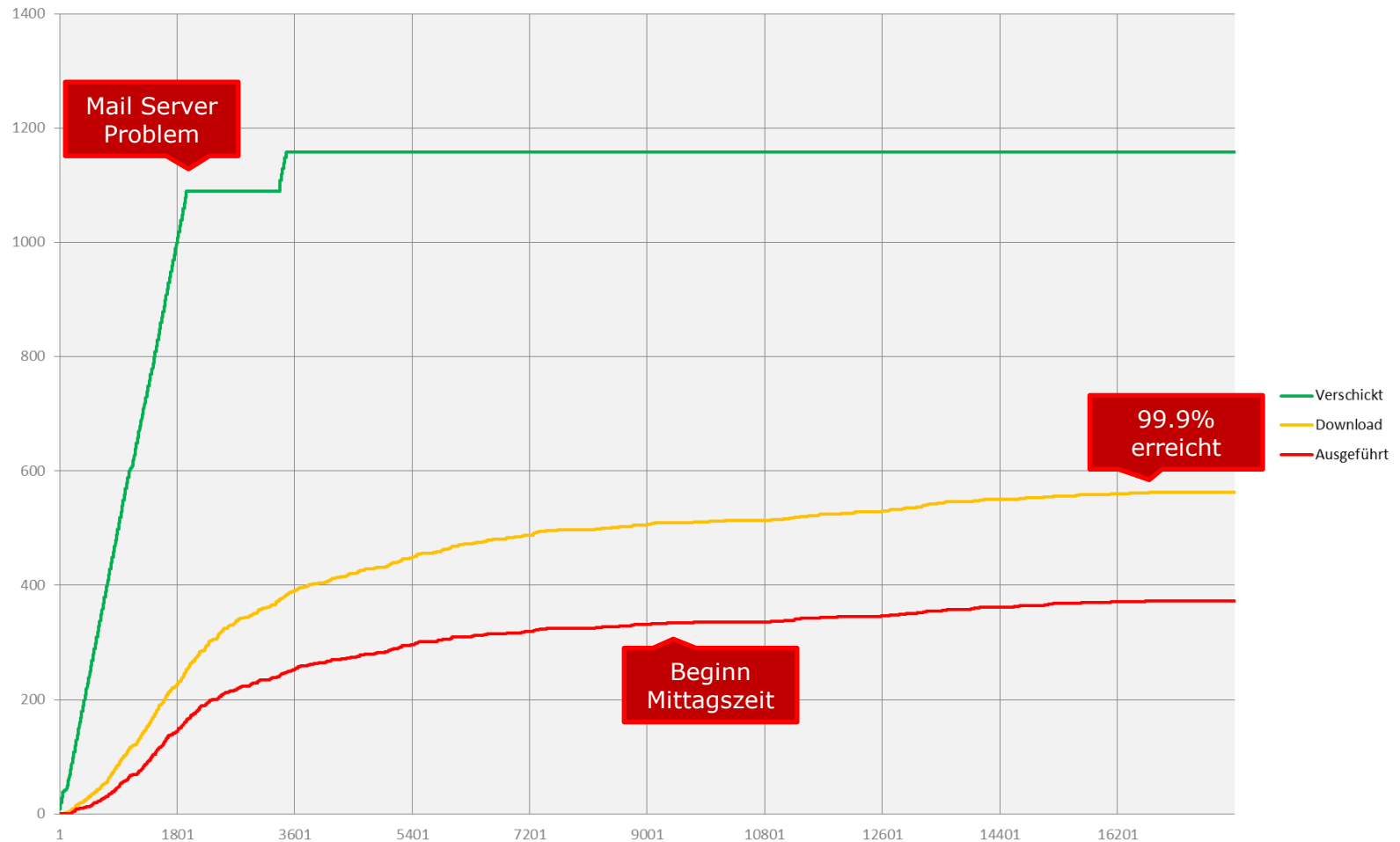
SQL ID	Mail Sent Timestamp UNIX	Mail Sent Timestamp Real	Download Timestamp UNIX	Download Timestamp Real	Phishing Incubation Time (Minutes)	Execution	Execution Timestamp UNIX	Execution Timestamp Real	Execution Incubation Time (Second)	Remote Address	Internal Hostname	Windows Username	Installed Path	Web Browser
1	1164183449	22.11.2006 09:17	1164183552	22.11.2006 09:19	2									
3	1164183449	22.11.2006 09:17												
4	1164183449	22.11.2006 09:17												
5	1164183449	22.11.2006 09:17	1164183520	22.11.2006 09:18	1	1	1164183538	22.11.2006 09:18	18					Microsoft Internet Explorer
6	1164183449	22.11.2006 09:17												
7	1164183449	22.11.2006 09:17	1164184391	22.11.2006 09:33	16	1	1164184407	22.11.2006 09:33	16					Other
8	1164183449	22.11.2006 09:17	1164183879	22.11.2006 09:24	7									
9	1164183449	22.11.2006 09:17	1164183653	22.11.2006 09:20	3									
10	1164183449	22.11.2006 09:17	1164186364	22.11.2006 10:06	49	1	1164186375	22.11.2006 10:06	11					Microsoft Internet Explorer
11	1164183465	22.11.2006 09:17												
12	1164183465	22.11.2006 09:17	1164183742	22.11.2006 09:22	5	1	1164183745	22.11.2006 09:22	3					Microsoft Internet Explorer
13	1164183465	22.11.2006 09:17	1164185211	22.11.2006 09:46	29	1	1164185219	22.11.2006 09:46	8					Microsoft Internet Explorer
14	1164183465	22.11.2006 09:17												
15	1164183465	22.11.2006 09:17												
16	1164183465	22.11.2006 09:17												
17	1164183465	22.11.2006 09:17												
18	1164183465	22.11.2006 09:17												
19	1164183465	22.11.2006 09:17	1164186472	22.11.2006 10:07	50									
20	1164183466	22.11.2006 09:17	1164188112	22.11.2006 10:35	77	1	1164188121	22.11.2006 10:35	9					Microsoft Internet Explorer
21	1164183481	22.11.2006 09:18												
22	1164183481	22.11.2006 09:18												
23	1164183481	22.11.2006 09:18												
24	1164183481	22.11.2006 09:18	1164186809	22.11.2006 10:13	56	1	1164186817	22.11.2006 10:13	8					Microsoft Internet Explorer
25	1164183481	22.11.2006 09:18	1164196762	22.11.2006 12:59	221									
26	1164183481	22.11.2006 09:18	1164197401	22.11.2006 13:10	232	1	1164197406	22.11.2006 13:10	5					Microsoft Internet Explorer
27	1164183481	22.11.2006 09:18												
28	1164183481	22.11.2006 09:18	1164183514	22.11.2006 09:18	1	1	1164185880	22.11.2006 09:58	2366					Microsoft Internet Explorer
29	1164183482	22.11.2006 09:18	1164185406	22.11.2006 09:50	32									
30	1164183482	22.11.2006 09:18	1164186679	22.11.2006 10:11	53									
31	1164183497	22.11.2006 09:18												
32	1164183497	22.11.2006 09:18	1164186347	22.11.2006 10:05	48	1	1164186354	22.11.2006 10:05	7					Microsoft Internet Explorer
33	1164183498	22.11.2006 09:18	1164183818	22.11.2006 09:23	5	1	1164183822	22.11.2006 09:23	4					Microsoft Internet Explorer
34	1164183498	22.11.2006 09:18	1164190754	22.11.2006 11:19	121									
35	1164183498	22.11.2006 09:18												
36	1164183498	22.11.2006 09:18												
37	1164183499	22.11.2006 09:18	1164189209	22.11.2006 10:53	95	1	1164189244	22.11.2006 10:54	35					Microsoft Internet Explorer
38	1164183499	22.11.2006 09:18	1164183726	22.11.2006 09:22	4									
39	1164183499	22.11.2006 09:18												
40	1164183499	22.11.2006 09:18	1164183593	22.11.2006 09:19	2									
41	1164183514	22.11.2006 09:18	1164183635	22.11.2006 09:20	2	1	1164183642	22.11.2006 09:20	7					Microsoft Internet Explorer
42	1164183524	22.11.2006 09:18	1164187094	22.11.2006 10:18	60	1	1164187098	22.11.2006 10:18	4					Microsoft Internet Explorer
43	1164183525	22.11.2006 09:18												
44	1164183542	22.11.2006 09:19												
45	1164183555	22.11.2006 09:19												
46	1164183561	22.11.2006 09:19	1164184477	22.11.2006 09:34	15	1	1164184492	22.11.2006 09:34	15					Microsoft Internet Explorer
47	1164183562	22.11.2006 09:19												
48	1164183563	22.11.2006 09:19	1164184227	22.11.2006 09:30	11	1	1164184229	22.11.2006 09:30	2					Microsoft Internet Explorer
49	1164183563	22.11.2006 09:19												
50	1164183564	22.11.2006 09:19												
51	1164183580	22.11.2006 09:19				1	1164186990	22.11.2006 10:16						Microsoft Internet Explorer



Nachbearbeitung | Typische Infektionsrate



Nachbearbeitung | Typischer Infektionsverlauf



Nachbearbeitung | Trivia

- Phishing
 - Erster Link-Klick nach 65 Sekunden
- Malware
 - Erste Infektion nach 89 Sekunden
 - Durchschnittliche Infektion nach 41.6 Minuten
 - Download-Versuche pro Infektion: 1.6 Mal
 - Download-Versuche maximal: 6 Mal



Nachbearbeitung | Reporting (Beispiel Massnahmenkatalog)

Element	Risiko	Massnahme
Awareness	High	Regelmässige Schulungen der Mitarbeiter
Mail Gateway	Medium	Phishing Detection Threshold optimieren
Web Proxy	High	Download von Binaries verhindern
Web Proxy	Low	Grösse ausgehender POST-Requests einschränken (<5MB)
Betriebssystem	High	Administrative Konten deaktivieren, nur noch Benutzer
Betriebssystem	High	Zusätzliche Antiviren-Lösung installieren
Logging	Medium	Zugriffe auf Shares zentralisiert protokollieren
...		



Abschluss | Zusammenfassung

- Backdoor Tests sind sehr effizient
- Mit ihnen kann die gesamtheitliche Sicherheit getestet werden
- Eine professionelle Umsetzung erfordert sehr viel Aufwand
- Der grösste Aufwand liegt in Entwicklung und Testing
- Die Erfolgsrate ist naturgemäss hoch



Abschluss | Dienste haben auch ein Interesse ...

"Am Computer des Täters ansetzen"

BKA-Präsident Jörg Ziercke findet es richtig, dass die Polizei heimlich Computer durchsuchen will. Denn nur so erhalte man die Daten, bevor der Täter sie verschlüsselt hat. Maßnahme komme "nur bei schwersten Straftaten" zum Einsatz

Der Staat als Einbrecher: Heimliche Online-Durchsuchungen sind möglich

Volker Birk 03.03.2007

Wie der geplante Bundestrojaner technisch funktionieren und wie man sich gegen ihn schützen könnte

Bürgerrechtler diskutieren mit BKA-Chef über Online-Durchsuchung

 vorlesen / MP3-Download

Zum Auftakt der Jahreskonferenz der [Humanistischen Union](#) diskutierten die Bürgerrechtler in einem Hörsaal der Universität Hannover mit Jörg Ziercke, dem Chef des Bundeskriminalamtes über die [umstrittene heimliche Online-Durchsuchung](#). Dabei prallten juristische und polizeitaktische Argumente ziemlich unvermittelt aufeinander.

Kommissar Trojaner

 vorlesen / MP3-Download

Während das Abhören von herkömmlichen Telefonaten in Fest- oder Mobilfunknetzen zum Tagesgeschäft gehört, stellen Verbindungen per Voice-over-IP für Strafermittler häufig ein Problem dar, besonders wenn überwachte Personen Skype über ausländische Server nutzen oder direkt von PC zu PC telefonieren und dabei die Daten verschlüsseln. Das Schweizer Departement für Umwelt, Verkehr und Kommunikation ([UVEK](#)) testet daher den Einsatz von Spionagesoftware, mit deren Hilfe sich die Gespräche auf den PCs der Kommunikationspartner abhören lassen sollen.

Hacken für den Staat

Polizei und Geheimdienst wollen Computer ausspähen. Womöglich sind nicht die juristischen Hürden das Problem, sondern die technischen. VON LUTZ HERKNER

Online-Durchsuchungen: Bundes-Trojaner sind spähbereit

Von Konrad Lischka

Das Bundeskriminalamt hat offenbar einen Computer-Trojaner fertiggestellt, der beliebige Rechner aus der Ferne durchsuchen kann. Das geht aus jetzt enthüllten Schreiben des Innenministeriums hervor. Der Bundes-Trojaner soll sogar Mobilgeräte ausspionieren können.



Abschluss | Fragen



Security Is Our Business!

scip AG

Jakob-Fügli-Strasse 18

CH-8048 Zürich

Tel +41 44 404 13 13

Fax +41 44 404 13 14

Mail info@scip.ch

Web <http://www.scip.ch>

Twitter <http://twitter.com/scipag>



- ☑ Strategy | Consulting
- ☑ Auditing | Testing
- ☑ Forensics | Analysis

