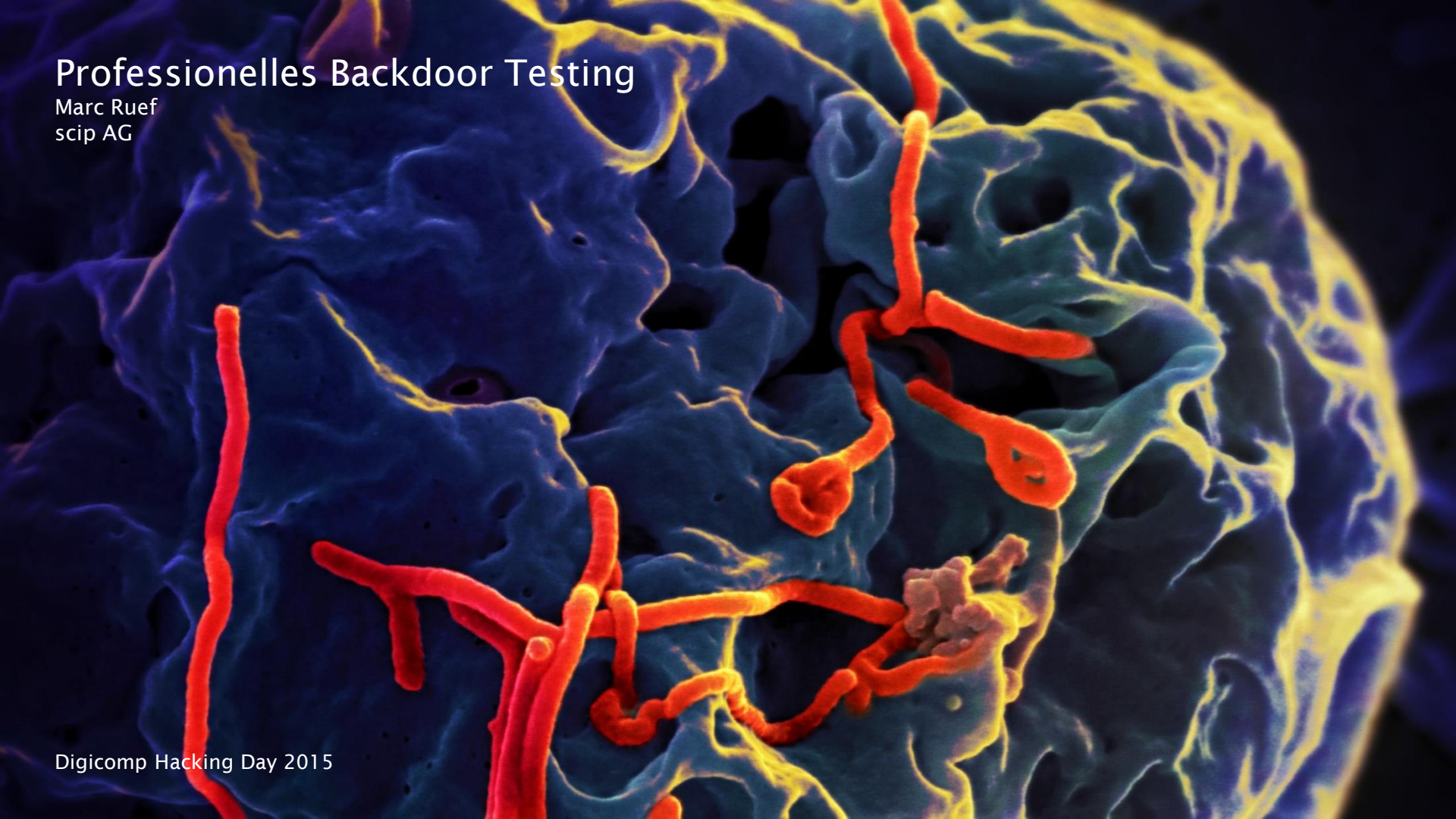
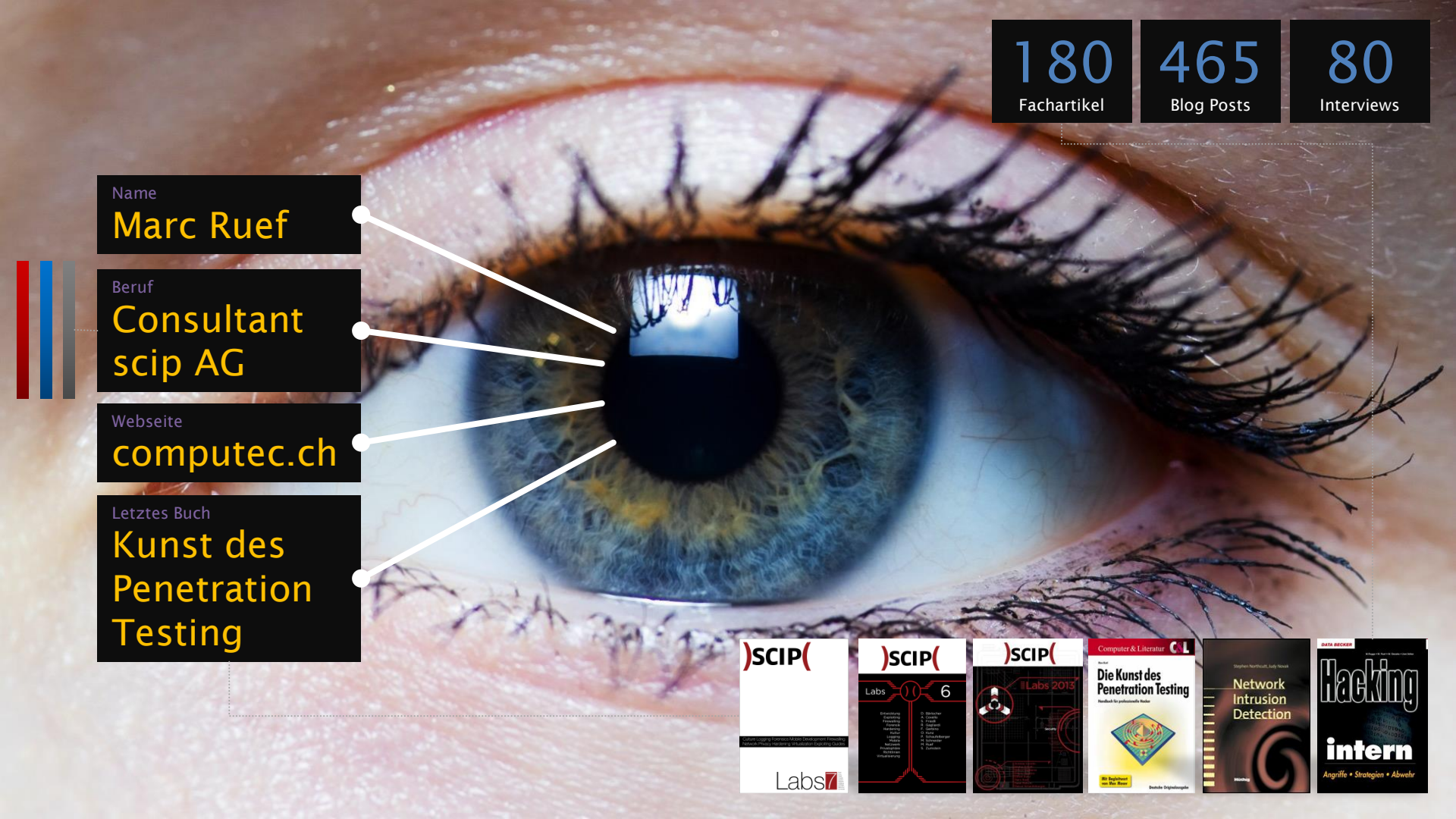
Professionelles Backdoor Testing

Marc Ruef
scip AG



Digicomp Hacking Day 2015


180
Fachartikel
465
Blog Posts
80
Interviews
Name
Marc Ruef
Beruf
Consultant
scip AG
Webseite
computec.ch
Letztes Buch
Kunst des
Penetration
Testing
)SCIP(
Labs7
)SCIP(
Labs
6
)SCIP(
Labs 2013
Computer & Literatur
Die Kunst des
Penetration Testing
Network
Intrusion
Detection
DATA BECKER
Hacking
intern
Angriffe • Strategien • Abwehr

Sicherheitsüberprüfungen sollen Schwachstellen aufdecken. Backdoor Tests sind eine spezielle Form von Prüfungen. Durch kundenspezifische Malware werden sämtliche Facetten des Sicherheitsdispositivs geprüft.

AWARENESS

WIE GEHEN BENUTZER MIT TECHNISCHEN ANGRIFFEN UND PSYCHOLOGISCHEN MANIPULATIONEN UM

MAIL SECURITY

WIE VERHÄLT SICH EIN ÜBER EMAIL INITIIERTER UND DURCHGESETZTER ANGRIFF AUF DAS UNTERNEHMEN

WEB SECURITY

WIE VERHÄLT SICH EIN ÜBER DAS WEB INITIIERTER UND DURCHGESETZTER ANGRIFF AUF DAS UNTERNEHMEN

FIREWALLS

KÖNNEN FIREWALL-KOMPONENTEN DIE UNERLAUBTEN ZUGRIFE ERKENNEN UND VERHINDERN

INCIDENT RESPONSE

FINDET EINE ZEITNAHE UND UMFASSENDE REAKTION AUF DEN ANGRIFFSVERSUCH STATT, UM DIESEN ZU UNTERBINDEN

ANTIVIRUS-LÖSUNGEN

KÖNNEN DIE ANTIVIREN-LÖSUNGEN MALWARE ALS SOLCHE ERKENNEN UND VERHINDERN

ALERTING

FINDET EINE ALARMIERUNG DER ENTSPRECHENDENSTELLEN BEI DER IDENTIFIKATION DES ANGRIFFS STATT

IDS

KÖNNEN INTRUSION DETECTION SYSTEME DEN ANGRIFFSVERSUCH ALS SOLCHEN ERKENNEN UND MELDEN

LOGGING

WERDEN DIE ANGRIFFE UND ZUGRIFFE FÜR WEITERE ANALYSEN ENTSPRECHEND PROTOKOLLIERT

DLP

KÖNNEN DIE EINGESETZTEN DATA LOSS PREVENTION MECHANISMEN DEN DATENABFLUSS ERKENNEN

IPS

KÖNNEN INTRUSION PREVENTION SYSTEME DEN ANGRIFF FRÜHZEITIG ALS SOLCHEN UNTERBINDEN

Zieldefinition

- Ausgangslage
  - Blackbox
  - Graybox
  - Whitebox
- Eintrittspunkt
  - Internet
  - DMZ
  - Partner-Anbindung
  - VPN
  - Intranet
  - LAN
- Angriffsvektor
  - Phishing
  - Email
  - Webbrowser
  - Host TCP/IP Stack
  - Cross Site Scripting
- Infektion
  - One-Shot
  - Temporär
  - Persistent
- ...
  - ...

Aspekt	Definition	Beschreibung
Ausgangslage	Whitebox	Es stehen uns sämtliche Details zur Zielumgebung zur Verfügung
Eintrittspunkt	Internet	Extern (nicht-authentisiert, nicht-priviligiert)
Angriffsvektor	Phishing + XSS	Es wird ein Phishing Email verschickt, das per Link auf die Firmenwebseite lockt. Dort wird durch eine bestehende XSS-Schwachstelle (in vorangegangenem Pentest gefunden) der Download eines SSL-Zertifikats vorgetäuscht.
Infektion	Temporär	Die Backdoor ist nur während der laufenden Sitzung aktiv. Spätestens ein Neustart deinstalliert sie.
Kommunikations-kanal	HTTPS	Über einen API Call wird eine HTTPS-Verbindung zum C&C Server 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 läuft und den Fokus hat. Weitere individuelle Datensammlungen über Queue möglich.
Lebensdauer	≤31.12.2015	Das Projekt läuft bis am 24.12.2015, wobei am letzten Tag manuell per Queue ein unload() initiiert wird. Eine Ausführung nach dem 31.12.2015 ist nicht mehr möglich.

```
var socket = 'socket.php';
var clientdebug = 0;
var xmlhttp = null;
var runnerinterval;
var interval = 5000;
var identifier;

function runner(){
    runnerinterval = setInterval("send_request(socket + '?request=QUERY&identifier=' + identifier, receive_command)", interval);
}

function send_request(url, onreadychange){
    xmlhttp = null;
    if(window.XMLHttpRequest){
        xmlhttp = new XMLHttpRequest();
    }else if(window.ActiveXObject){
        xmlhttp = new ActiveXObject('Microsoft.XMLHTTP');
    }
    if(xmlhttp != null){
        xmlhttp.onreadystatechange=onreadychange;
        xmlhttp.open('GET', url, true);
        xmlhttp.setRequestHeader('If-Modified-Since', 'Fri, 31 Dec 1999 23:59:59 GMT');
        xmlhttp.send(null);
    }else{
        clearInterval(runnerinterval);
        alert('Your browser does not support XMLHTTP.');
    }
}

function receive_command(){
    if(xmlhttp.readyState==4){
        if(xmlhttp.status==200){
            identifier = xmlhttp.responseXML.getElementsByTagName('identifier')[0].childNodes[0].nodeValue;
            var response = xmlhttp.responseXML.getElementsByTagName('response')[0].childNodes[0].nodeValue;

            if(clientdebug){
                var statuscode = xmlhttp.responseXML.getElementsByTagName('statuscode')[0].childNodes[0].nodeValue;
                var statustext = xmlhttp.responseXML.getElementsByTagName('statustext')[0].childNodes[0].nodeValue;
                var timestamp = xmlhttp.responseXML.getElementsByTagName('timestamp')[0].childNodes[0].nodeValue;
                var receiver = xmlhttp.responseXML.getElementsByTagName('receiver')[0].childNodes[0].nodeValue;
                show_debug('=> QUERY: ' + statuscode + ' (' + statustext + ') ' + timestamp + ' ' + identifier + ' ' + receiver + ' ' + response);
            }

```

Queue-Intervall 5 Sekunden

Runner fragt Queue ab

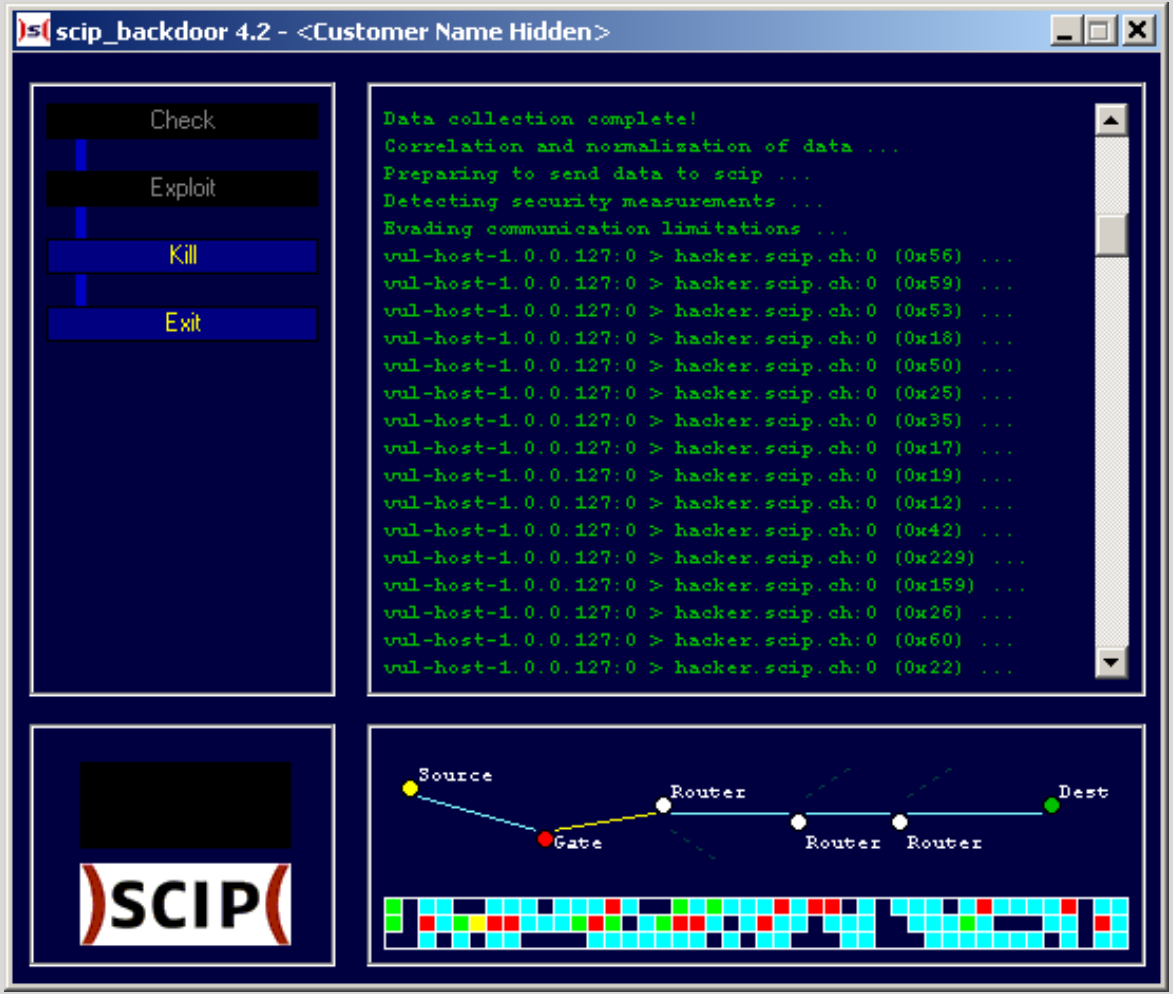
XMLHTTP als Mechanismus

Caching mit Header verhindern

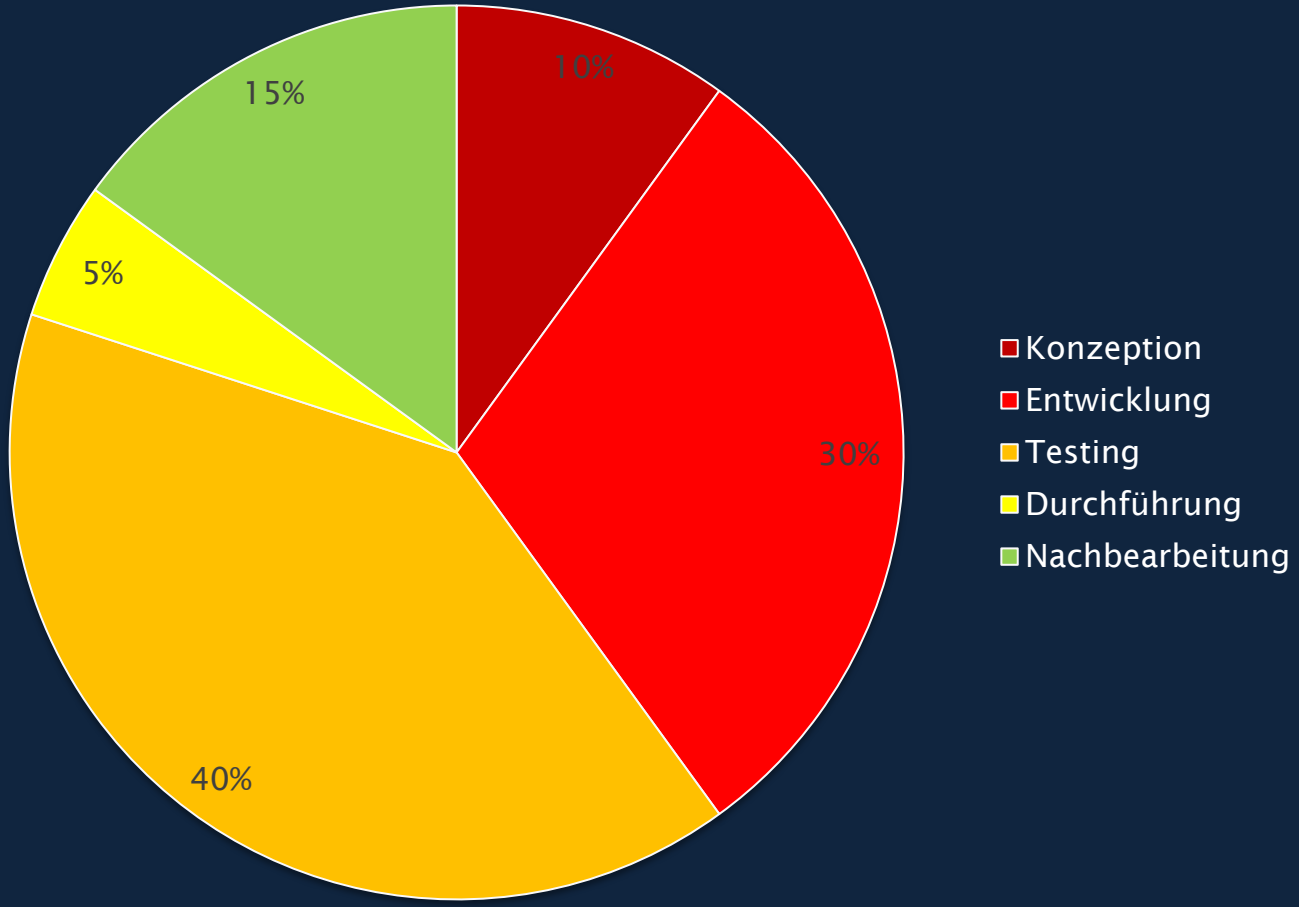
Elemente aus Response

Debug View aktivieren

VBA Backdoor transparentes Beispiel



Aufwände im Vergleich



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, ...


5 x 2 Tickets mit Swiss ab
Zürich Kloten nach New York.
3 Übernachtungen im Hotel
Affinia in Manhatten.
CHF 1000.– Taschengeld
4 TAGE SHOPPING
IN NEW YORK
HelveticTours
Ein Wettbewerb von Helvetic Tours
REZY
10163

Helvetic Tours Quiz

HelveticTours

Wie 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

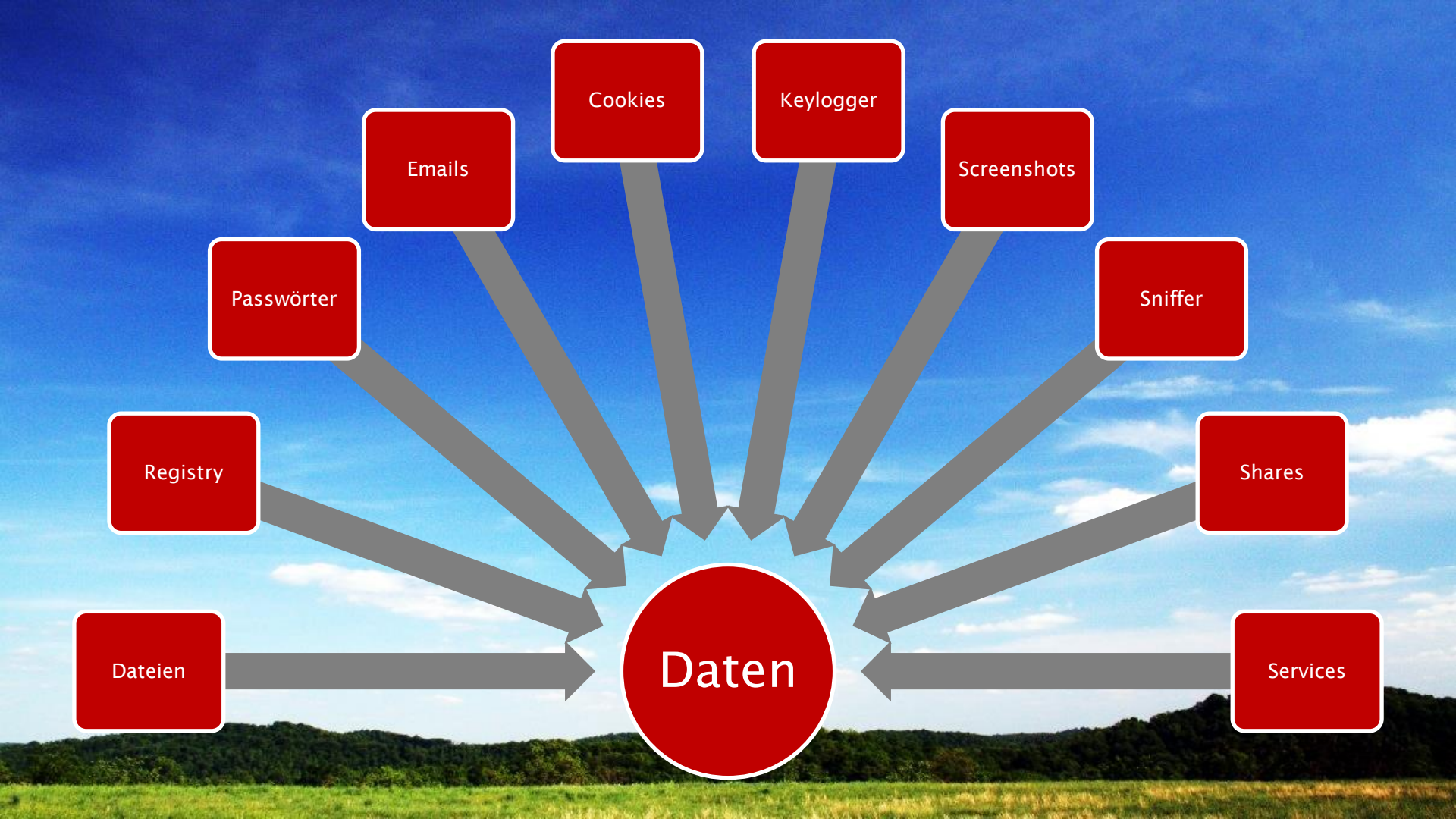
Welcher berühmte Entertainer hat New York ein Lied gewidmet?

- 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 schriftlich benachrichtigt. Die Preise können nicht bar ausbezahlt werden. Über den Wettbewerb wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Mitmachen & Gewinnen


Zielpersonen + Zielsysteme
müssen während des gesamten
Tests identifizierbar sein


Cookies
Keylogger
Emails
Screenshots
Passwörter
Sniffer
Registry
Shares
Dateien
Daten
Services

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 (langsam, zufällig, unüblich/üblich)

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 [individuell]
- Freigeben von Speicher [4-8 MB]
- Entfernen der Binaries [<0.5 MB]

Auswertung

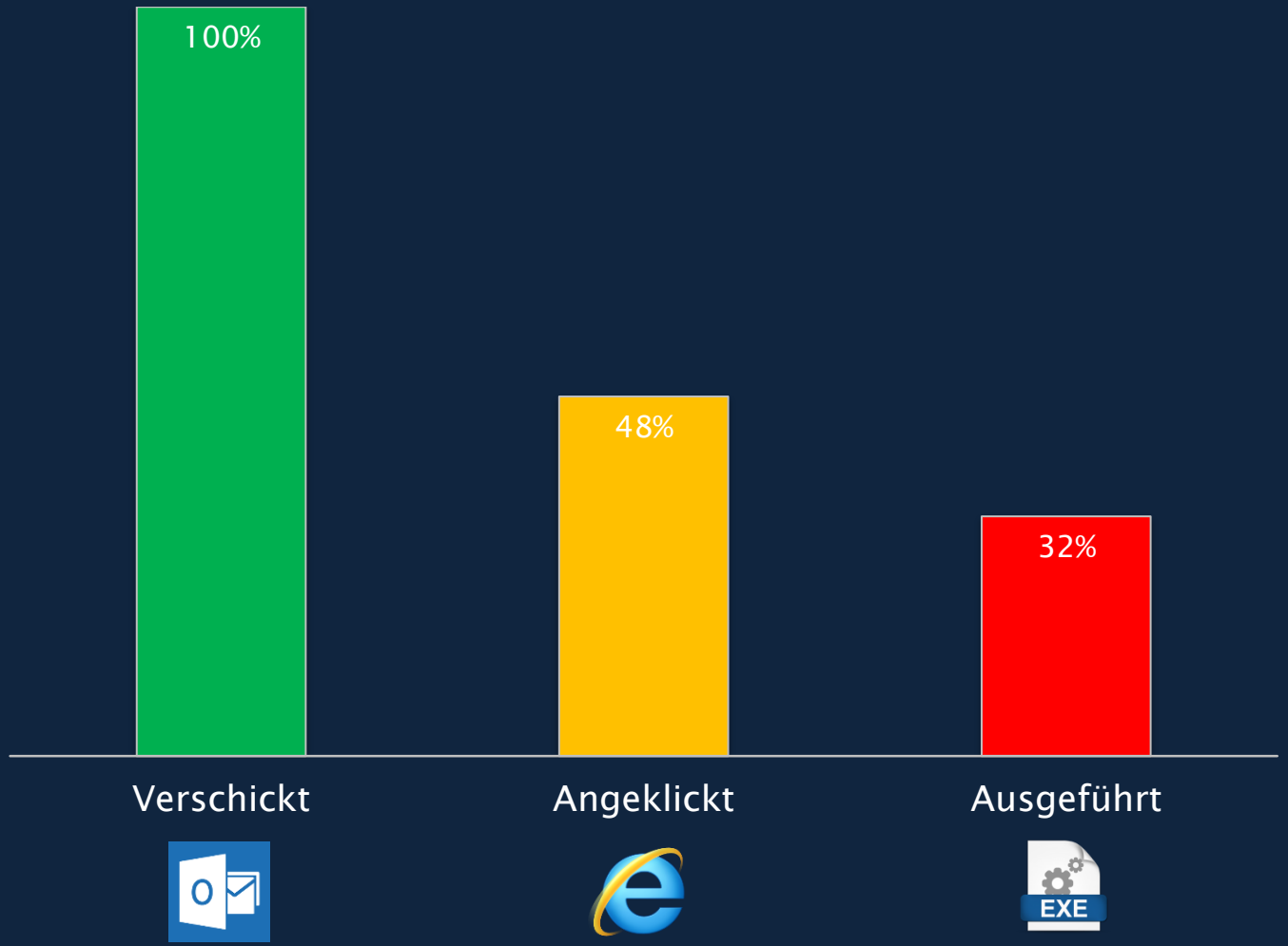
Infektionspfad muss pro Benutzer/System nachvollziehbar sein

- Email mit personenbezogener Mailadresse
- Webbug in Email mit personalisierter URL
- Download Link mit personalisierter URL
- Backdoor liefert Username/Hostname/IP-Adresse/MAC-Adresse

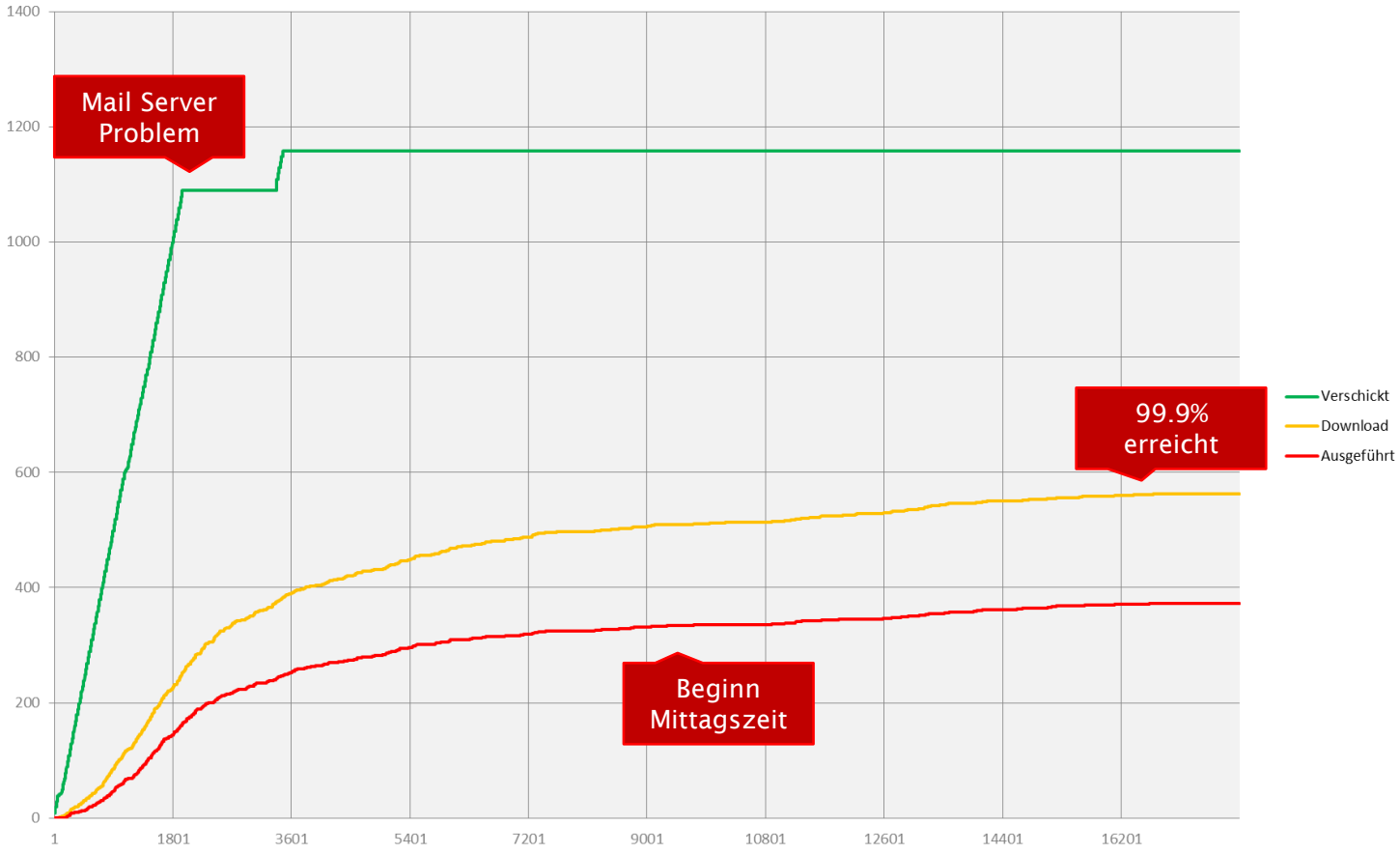
Personenbezogene Informationen werden **nicht** an den Kunden weitergegeben

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					[redacted]				
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	[redacted]				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	[redacted]				Other
8	1164183449	22.11.2006 09:17	1164183879	22.11.2006 09:24	7					[redacted]				
9	1164183449	22.11.2006 09:17	1164183653	22.11.2006 09:20	3					[redacted]				
10	1164183449	22.11.2006 09:17	1164186364	22.11.2006 10:06	49	1	1164186375	22.11.2006 10:06	11	[redacted]				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	[redacted]				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	[redacted]				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					[redacted]				
20	1164183466	22.11.2006 09:17	1164188112	22.11.2006 10:35	77	1	1164188121	22.11.2006 10:35	9	[redacted]				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	[redacted]				Microsoft Internet Explorer
25	1164183481	22.11.2006 09:18	1164196762	22.11.2006 12:59	221					[redacted]				
26	1164183481	22.11.2006 09:18	1164197401	22.11.2006 13:10	232	1	1164197406	22.11.2006 13:10	5	[redacted]				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	[redacted]				Microsoft Internet Explorer
29	1164183482	22.11.2006 09:18	1164185406	22.11.2006 09:50	32					[redacted]				
30	1164183482	22.11.2006 09:18	1164186679	22.11.2006 10:11	53					[redacted]				
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	[redacted]				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	[redacted]				Microsoft Internet Explorer
34	1164183498	22.11.2006 09:18	1164190754	22.11.2006 11:19	121					[redacted]				
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	[redacted]				Microsoft Internet Explorer
38	1164183499	22.11.2006 09:18	1164183726	22.11.2006 09:22	4					[redacted]				
39	1164183499	22.11.2006 09:18												
40	1164183499	22.11.2006 09:18	1164183593	22.11.2006 09:19	2					[redacted]				
41	1164183514	22.11.2006 09:18	1164183635	22.11.2006 09:20	2	1	1164183642	22.11.2006 09:20	7	[redacted]				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	[redacted]				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	[redacted]				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	[redacted]				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		[redacted]				Microsoft Internet Explorer

Typische Infektionsrate



Typischr Infektionsverlauf



65

SEKUNDEN BIS ZUM ERSTEN ANKLICKEN DER VERSCHICKTEN LINKS

89

SEKUNDEN BIS ZUR ERSTEN ERFOLGREICHEN INFEKTION

41.6

MINUTEN BRAUCHT EINE ERFOLGREICHE INFEKTION IM DURCHSCHNITT

1.6

MAL WIRD IM SCHNITT DER DOWNLOAD VERSUCHT

6

MAL VERSUCHTE DAS HARTNÄCKIGSTE OPFER DEN DOWNLOAD

Massnahmenkatalog

Element	Risiko	Massnahme
Mitarbeiter	High	Regelmässige Awareness Schulungen
Mail Gateway	Medium	Phishing Detection Threshold optimieren
Web Proxy	High	Download von Binaries verhindern
Web Proxy	Low	Grösse ausgehender POST-Requests einschränken (<5MB)
Firewall	High	Keine ANY Rules Richtung DMZ zulassen
Betriebssystem	High	Administrative Konten deaktivieren, nur noch Benutzer
Betriebssystem	High	Zusätzliche hostbasierte Antiviren-Lösung installieren
Betriebssystem	Medium	Zugriffe auf externe Datenträger einschränken
Logging	Medium	Zugriffe auf Shares zentralisiert protokollieren
Alerting	Medium	Alarmierung zusätzlich per SMS auslösen
...		

BACKDOOR TESTING

EFFIZIENTES MITTEL ZUR IDENTIFIKATION VON SCHWACHSTELLEN

Erfolgreiche Kompromittierung der Zielumgebung durch die Infektion eines eigens angefertigten Trojanischen Pferds zur Bestimmung effektiv ausnutzbarer Schlupflöcher im bestehenden Sicherheitsdispositiv.

Backdoor Tests sind sehr individuell. Primär in Prosaform werden die Vorbereitungen (Entwicklung der Hintertür) sowie die Durchführung des Angriffs (Infektion und Fernsteuerung) dokumentiert. Dabei wird Schritt für Schritt aufgezeigt, wie die Attacke durchgeführt wurde. Die ausgenutzten Schwächen der Zielumgebung (z.B. Firewall-Tunneling, Antivirus Evasion, etc.) und/oder der involvierten Personen (z.B. Social Engineering, Phishing, etc.) werden ausführlich besprochen.

)SCIP(

scip AG
Badenerstrasse 623
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
☑ Research | Analysis

Bildquellen:

Virus: NIAID, https://www.flickr.com/photos/niaid/14712446017
Eye: Laitr Keiows, https://commons.wikimedia.org/wiki/File:Iris_-_right_eye_of_a_girl.jpg
Ammunition: Ninjatoth, https://commons.wikimedia.org/wiki/File:Various_Ammunition.jpg
Bacteria: NIAID, https://www.flickr.com/photos/niaid/16578744517
Camera Lens: jarmoluk, https://pixabay.com/en/lens-sigma-17-50-zoom-photo-736109/
Faces: Lauren Manning, https://www.flickr.com/photos/laurenmanning/2395336559
Sky: ForestWander, https://commons.wikimedia.org/wiki/File:Sky-View_ForestWander.JPG
Camouflage: free photos, https://www.flickr.com/photos/79818573@N04/15421951588
Water: okbrightstar-stock, http://okbrightstar-stock.deviantart.com/art/Water-Texture-7-142314119
Snow: Nick Mealey, https://www.flickr.com/photos/nickmealey/8374772757
Sword: Søren Niedziella, https://commons.wikimedia.org/wiki/File:Albion_Baron_Medieval_Sword_4_(6091866751).jpg