

Contents

1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Statistiken Verletzbarkeiten
5. Labs
6. Bilderrätsel
7. Impressum

1. Editorial

Infiltration eines Netzwerks

Ein krimineller Angriff auf ein Computersystem umfasst unterschiedliche Phasen. Will man die Nennung dieser möglichst reduzieren, so kann man sich auf (1) Auswertung, (2) Angriff, (3) Kompromittierung, (4) Rechteausweitung und (5) Backdooring einigen. Eine überproportional hohe Anzahl an Fachpublikationen beschäftigt sich mit dem Einbrechen in Computersysteme, also mit den Phasen 1 bis 3. Auch im Rahmen von professionellen Sicherheitsüberprüfungen wird anhand dieser in erster Linie die Machbarkeit eines Angriffs bewiesen und anhand dem Erfolg dieser die Durchführbarkeit der restlichen zwei Phasen abgeleitet.

Nur in den wenigsten Fällen werden die Hürden, wie sie mit einer Rechteausweitung und einem Backdooring verbunden sind, berücksichtigt. Doch die meisten Angreifer attackieren Systeme heutzutage nicht mehr nur aus Spass, sondern sie wollen einen Nutzen aus ihren Aktivitäten davontragen. Der Nutzen erschliesst sich aber erst dann, wenn Zugriffe auf Daten und Systemressourcen durchgesetzt werden können. Die Möglichkeiten der Phasen 4 und 5 sind entsprechend massgeblich dafür verantwortlich, welches Ausmass an Erfolg der gesamte Angriffsversuch mit sich zu bringen in der Lage ist.

Gehen wir davon aus, dass jemand in ein Netzwerk einbrechen möchte, um aus diesem Daten zu stehlen. Das Zielunternehmen bietet ein WLAN an, das durch bekannte Angriffstechniken innert weniger Stunden kompromittiert werden kann. Das System des Angreifers wird nach erfolgreicher Anmeldung im WLAN zu einem Teil des bestehenden Netzwerks.

Als erstes wird der Angreifer versuchen herauszufinden, wie das Netzwerk konfiguriert ist. Anhand der DHCP-Einstellungen, die automatisch an sein System propagiert wurden, kann er erste Ableitungen zu IP-Adressierung durchführen. Handelt es sich um ein Klasse C- oder ein Klasse A-Netzwerk, können Rückschlüsse auf die Grösse des Unternehmens und die potentiellen Angriffsziele (im gleichen Netzwerksegment) gemacht werden.

Wird dem eigenen System die IP-Adresse 192.168.2.51 zugeordnet, so kann in einem nächsten Schritt versucht werden herauszufinden, ob die inkrementelle Vergabe der IP-Adressen durch den DHCP-Server den gesamten Adressraum von 1-50 aufbraucht und ob ebenfalls Adressen im Bereich >51 vergeben sind. Die Anzahl aktiver Systeme kann so ermittelt werden. Je nach Tageszeit lässt sich damit erkennen, wieviele Mitarbeiter in etwa zugegen sind (manche von ihnen werden hoffentlich unter Berücksichtigung von Green-IT ihr System über Nacht/Wochenende ausschalten).

Doch um die Belegbarkeit des Adressraums zu ermitteln, muss zuerst die Topologie des Netzwerks verstanden werden. Ebenfalls in den mit DHCP auferlegten Konfigurationseinstellungen kann das Default Gateway, die DNS-Server sowie der DHCP-Server erkannt werden. Das Gateway ist üblicherweise die niederwertigste IP-Adresse im Adressbereich (in diesem Fall 192.168.2.1). Der DHCP-Server nimmt für sich ebenfalls die gleiche IP-Adresse in Anspruch. Die Nameserver findet sich jedoch im Netzwerk 172.16.0.x. Es ist sodann anzunehmen, dass die Server-Systeme in eben dieser DMZ positioniert werden.

Durch das Einsehen der lokalen ARP-Tabelle

können die Ethernet-Adressen der schon angesprochenen Systeme ausgemacht werden. Die ersten drei hexadezimalen Werte lassen den Hersteller (Vendor) der Netzwerkkarte ermitteln. Schnell und vor allem passiv (keine weiteren Zugriffe für die Auswertung nötig) lässt sich damit ausmachen, dass das Gateway mit grösster Wahrscheinlichkeit durch ein Cisco-Gerät bereitgestellt wird. Die Namensauflösung lässt eine Cisco PIX/ASA vermuten (wiederum eine indirekte Auswertung). Dadurch kann die zur Filterung eingesetzte Technologie abgeleitet und potentiell verdächtige Aktivitäten zurückgehalten werden.

Anhand der weiterführenden Namensauflösungen der Systeme im gleichen Netzwerksegment lässt sich eine ISS RealSecure-Installation ausmachen. Hierbei handelt es sich um ein kommerzielles Intrusion Detection-System (IDS). Da die ersten langsamen Portscans der Client-Systeme typische Standard-Installationen von Windows XP erkennen liess, wird ebenfalls eine Standard-Installation von RealSecure erwartet. Mit der Durchsicht dieser in einer eigenen Test-Installation kann erkannt werden, welche Aktivitäten voraussichtlich Alarm auslösen werden. Das eigene Verhalten kann damit massgeblich optimiert werden, um unentdeckt weiter vorzugehen.

Da die gegebenen Windows-Systeme kein aktuelles Patch-Level aufweisen, kann mit einem mehr oder weniger bekannten Exploit eine Kompromittierung eines solchen angestrebt werden. Die Auswertung der Konfigurationseinstellungen (die erste Kompromittierung hat lediglich die Rechte des eingeloggten Benutzers vererben lassen), lässt File-Server und versteckte Shares erkennen. Auf diese können nun zugegriffen werden, wobei nach wertvollen Daten sowie technischen Hinweisen zur Umgebung Ausschau gehalten wird.

Die Durchsicht des File-Servers lässt im Ordner \IT-Department\Networking\Diagrams Visio-Dokumente identifizieren, die die Architektur und Topologie des gesamten Firmennetzwerks dokumentieren. Auf einen Blick werden so sämtliche Netzwerkzonen, Übergänge (Router/Firewalls), Server und Systeme erkennbar. Dank dieser "Landkarte" kann man sich nun sehr effizient im Netzwerk bewegen und kann deshalb auf eine Vielzahl an langwierigen Auswertungen (z.B. Erkennen der existenten/erreichbaren Systeme mittels Ping-Suchlauf) verzichten.

Nun kann entweder versucht werden durch ein lokales Exploiting die Rechte auf dem kompromittierten Arbeitsplatzrechner zu erweitern. Dies ist wohl nicht weiter erforderlich, da mit administrativen Rechten nur marginal erweiterte Zugriffe mit zusätzlichem Nutzen angegangen werden können. Eine Rechteauserweiterung ist eigentlich nur dann angestrebt, wenn die zusätzlichen Privilegien für die gewünschten Zugriffe erforderlich sind (z.B. Zugriff auf Systemkomponenten, Missbrauch einer bestehenden Vertrauensbeziehung im Netzwerk).

Oder man fokussiert sich auf die elementaren und damit wertvollsten Systeme der Zielumgebung. Vor allem Routing-, Security- und zentrale Server-Systeme sind von Interesse. Da diese ein Mehr an Funktionen bereitstellen und Kommunikationen bearbeiten, kann eine Übernahme dieser ein Mehr an Möglichkeiten gewähren (z.B. könnte ein manipulierter Proxy sämtlichen Verkehr auf das eigene System umleiten und durch eine klassische Man-in-the-Middle Attacke den Datenstrom mitlesen lassen). Der weitere Angriff dieser Systeme ist nun jedoch wieder als neu gestartete Iteration der fünf Phasen zu verstehen. Nach dem Angriff ist vor dem Angriff.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 28. Juni 2010

2. scip AG Informationen

2.1 Security Coaching

Das Ziel des Security Coaching ist die direkte Beratung und das unmittelbare Coaching des Kunden in den Bereichen der Information Security zur Sicherstellung nachhaltiger und sicherer Prozesse, Architektur- und Technologieentscheidungen.

Der Kunde bespricht mit uns seine Ziele und Vorgaben. Anhand dessen unterstützen wir den Kunden mit unserer fachmännischen Expertise und langjährigen Erfahrung im Security Bereich. Bei Sitzungen mit Partnern stellen wir das entsprechende Know-How zur Formulierung wichtiger Nachfragen zur Verfügung.

- Vorbereitung: Zusammentragen aller vorhandenen Informationen zur anstehenden Aufgabe.
- Research: Einholen von weiteren Informationen (z.B. Erfahrungen von anderen Kunden).
- Diskussion: Besprechung der Aufgabe und der daraus resultierenden Möglichkeiten.
- Empfehlung: Aussprechen und Dokumentieren eines vertretbaren Lösungswegs.

In erster Linie soll in beratender Weise eine direkte Hilfestellung mit konkreten Empfehlungen und Lösungen bereitgestellt werden. Eine Dokumentation (Protokolle, Kommunikationsmatrizen, Statements etc.) erfolgt auf Wunsch des Kunden.

Durch die direkte Beteiligung an einem Projekt kann unmittelbar Einfluss ausgeübt, damit die Etablierung schwerwiegender Fehler verhindert und ein Höchstmass an Sicherheit erreicht werden. Da Sicherheit von Beginn an zur Diskussion steht, lassen sich Schwachstellen von vornherein vermeiden. Aufwendigen Tests und nachträgliche Anpassungen können so vorgebeugt werden.

Dank unserer langjährigen Erfahrung und unserem ausgewiesenen Expertenwissen konnten wir als scip AG bereits eine grosse Anzahl an Kunden beraten und begleiten.

Zählen auch Sie auf uns!

<http://www.scip.ch/?firma.referenzenalle>

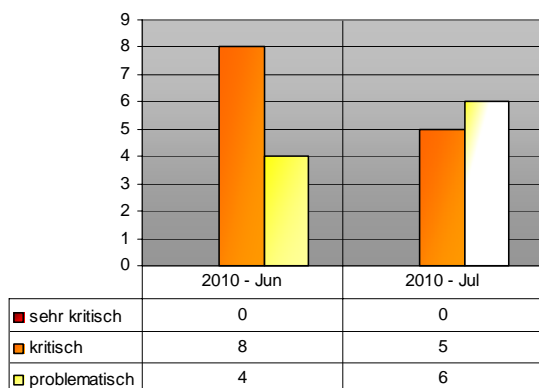
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an chris.widmer@scip.ch.

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/?vuldb> einsehbar.



Die Dienstleistungspakete scip(pallas liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.



Contents:

- 4154 Cisco Industrial Ethernet 3000 Hardcoded SNMP Community Names
- 4152 Microsoft Windows MFC Document Title Updating Pufferüberlauf
- 4151 Microsoft Windows NtUserCheckAccessForIntegrityLevel Use-After-Free Schwachstelle
- 4150 Citrix XenServer Denial of Service
- 4149 Microsoft Windows Shell Shortcut Parsing Schwachstelle
- 4148 BIND "RRSIG" Requests Endless Loop Denial of Service
- 4146 Microsoft Office Outlook Linked Attachment Verification Schwachstelle
- 4145 Microsoft Office Access ActiveX Controls zwei Schwachstellen
- 4144 Winamp VP6 Content Parsing Integer Overflow
- 4143 Shemes Grabit Malicious NZB Date Denial of Service
- 4142 Skype Client für Mac Chat Unicode Denial of Service

3.1 Cisco Industrial Ethernet 3000 Hardcoded SNMP Community Names

Risiko: **kritisch**

Remote: Ja

Datum: 08.07.2010

scip DB: <http://www.scip.ch/?vuldb.4154>

Cisco Systems, Inc. ist ein US-amerikanisches Unternehmen aus der Telekommunikationsbranche. Bekannt ist es vor allem für seine Router und Switches, die einen großen Teil des Internet-Backbones versorgen. Die Firma Cisco identifizierte unlängst eine Schwachstelle (Designfehler) in aktuellen Versionen der vorliegenden Applikation. Durch die Verwendung fester, nicht veränderbarer SNMP Community Names kann ein Angreifer Daten aus dem Gerät extrahieren und möglicherweise erweiterte Rechte erlangen.

Expertenmeinung:

Die vorliegende Schwachstelle ist für den Hersteller Cisco bestenfalls als peinlich zu betrachten. Der Einsatz hardgecodeter SNMP Namen im Jahre 2010 rechtfertigt sicherlich eine derartige Taxierung. Betroffenen Benutzern wird das Einspielen einer aktualisierten Version empfohlen.

3.2 Microsoft Windows MFC Document Title Updating Pufferüberlauf

Risiko: **problematisch**

Remote: Ja

Datum: 05.07.2010

scip DB: <http://www.scip.ch/?vuldb.4152>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS). Inzwischen wurde dieser Entwicklungszweig zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Der Researcher f10 f10w veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Pufferüberlauf) in verschiedenen Versionen des Produktes beschreibt. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

Expertenmeinung:

Die vorliegende Schwachstelle ist, wie die meisten Schwächen dieser Art, als ungünstig zu betrachten. Das Einspielen entsprechender Patches ist als empfehlenswert zu betrachten.

3.3 Microsoft Windows NtUserCheckAccessForIntegrityLevel Use-After-Free Schwachstelle

Risiko: **problematisch**

Remote: Ja

Datum: 05.07.2010

scip DB: <http://www.scip.ch/?vuldb.4151>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS). Inzwischen wurde dieser Entwicklungszweig zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Ein Researcher der Microsoft-Spurned Researcher Collective (MSRC) beschreibt in einem Advisory eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der Applikation. Durch die Ausnutzung der vorliegenden Schwachstelle kann unter Umständen beliebiger Code zur Ausführung gebracht werden, was zur Kompromittierung des Systems führen kann.

Expertenmeinung:

Leider sind keine ausführlichen Details zur genannten Schwachstelle bekannt. Dadurch kann keine spezifische Empfehlung abgegeben werden.

3.4 Citrix XenServer Denial of Service

Risiko: **problematisch**

Remote: Ja

Datum: 29.06.2010

scip DB: <http://www.scip.ch/?vuldb.4150>

Citrix Systems ist ein US-amerikanisches Softwareunternehmen, das 1989 von Ed Iacobucci gegründet wurde und jetzt in Fort Lauderdale in Florida ansässig ist. Citrix-Aktien werden an der NASDAQ unter dem Kürzel CTXS gehandelt. Citrix Systems ist in 35 Ländern aktiv. Die Firma Sygard.no veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Denial of Service (DoS)) in verschiedenen Versionen des Produktes beschreibt. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of

Service Angriff erzeugen und damit den Betrieb des Systems und der entsprechenden Umsysteme empfindlich stören.

Expertenmeinung:

Die vorliegende DoS Schwachstelle ist zwar nicht als hochkritisch zu betrachten, kann aber je nach Umgebung ernsthafte Folgen nach sich ziehen. Das Einspielen eines entsprechenden Patches wird auch hier stark empfohlen.

3.5 Microsoft Windows Shell Shortcut Parsing Schwachstelle

Risiko: **kritisch**

Remote: Ja

Datum: 17.07.2010

scip DB: <http://www.scip.ch/?vuldb.4149>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS). Inzwischen wurde dieser Entwicklungszweig zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Die Firma Microsoft identifizierte unlängst eine, derzeit als 0-day im Umlauf befindliche, Schwachstelle (Designfehler) in aktuellen Versionen der vorliegenden Applikation. Durch die Ausnutzung der vorliegenden Schwachstelle kann unter Umständen beliebiger Code zur Ausführung gebracht werden, was zur Kompromittierung des Systems führen kann.

Expertenmeinung:

Die vorliegende Schwachstelle wird bereits sehr aktiv im Rahmen von Angriffen mit Speichermedien, wie zum Beispiel USB Sticks, angewandt. Bis ein Patch verfügbar ist, sollten die Workarounds des Herstellers in Betracht gezogen werden.

3.6 BIND "RRSIG" Requests Endless Loop Denial of Service

Risiko: **problematisch**

Remote: Ja

Datum: 16.07.2010

scip DB: <http://www.scip.ch/?vuldb.4148>

BIND (Berkeley Internet Name Domain, vormals auch -Daemon) ist ein Open-Source-Softwarepaket, mit dem auf Rechnern mit Standard-Betriebssystemen (z. B. UNIX,

NetBSD, FreeBSD, OpenBSD, Linux, Mac OS X, Windows NT, z/OS, OS/2) ein Domain-Name-System-Server implementiert werden kann. BIND kann kostenlos bezogen werden, der Quelltext ist veröffentlicht. Aufgrund seiner weiten Verbreitung und der zeitnahen Umsetzung der aktuellen DNS-RFCs gilt BIND seit Jahren als DNS-Referenzsoftware. Der Researcher Marco Davids der Firma SIDN veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Denial of Service (DoS)) in verschiedenen Versionen des Produktes beschreibt. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und - unter Umständen - beliebigen Code zur Ausführung bringen.

Expertenmeinung:

Schwachstellen in DNS Servern sind grundsätzlich als ungünstig zu betrachten. Im vorliegenden Fall kann die Kritikalität als etwas reduziert betrachtet werden, dennoch sollte zeitnah ein Patch zum Einsatz gebracht werden.

3.7 Microsoft Office Outlook Linked Attachment Verification Schwachstelle

Risiko: **kritisch**

Remote: Ja

Datum: 13.07.2010

scip DB: <http://www.scip.ch/?vuldb.4146>

Microsoft Office ist das Office-Paket des US-amerikanischen Unternehmens Microsoft für die Betriebssysteme Microsoft Windows und Mac OS X. Für unterschiedliche Aufgabenstellungen werden verschiedene Suiten angeboten, die sich in den enthaltenen Komponenten, dem Preis und der Lizenzierung unterscheiden. Der Researcher Yorick Koster der Firma Akita Software Security beschreibt in einem Advisory eine Schwachstelle (Umgehungs-Angriff) in aktuellen Versionen der Applikation. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

Expertenmeinung:

Durch die geschickte Ausnutzung von Schwächen in der PR_ATTACH_METHOD Methode kann hier beliebiger Code zur Ausführung gebracht werden. Anwender, die eine verwundbare Version einsetzen, sind mit dem zeitnahen Einspielen des entsprechenden Patches gut beraten.

3.8 Microsoft Office Access ActiveX Controls zwei Schwachstellen

Risiko: **kritisch**

Remote: Ja

Datum: 13.07.2010

scip DB: <http://www.scip.ch/?vuldb.4145>

Microsoft Access (kurz MS Access, nach engl. access, "Zugang"), ist ein proprietäres Datenbankmanagementsystem der Firma Microsoft zur Verwaltung von Daten in Datenbanken und zur Entwicklung von Datenbankanwendungen. MS Access ist Bestandteil des Office-Professional-Pakets und unterstützt (mit Einschränkungen) SQL-92. Ein Researcher der ZDI veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Pufferüberlauf) in verschiedenen Versionen des Produktes beschreibt. Ein Angreifer kann durch die vorliegende Schwachstelle beliebigen Code zur Ausführung bringen und somit die Kompromittierung des Systems anstreben.

Expertenmeinung:

Die vorliegenden Schwachstellen müssen zum jetzigen Zeitpunkt als kritisch betrachtet werden und sollten durch das Einspielen entsprechender Patches zeitnah behoben werden.

3.9 Winamp VP6 Content Parsing Integer Overflow

Risiko: **kritisch**

Remote: Ja

Datum: 13.07.2010

scip DB: <http://www.scip.ch/?vuldb.4144>

Winamp ist ein unter Windows verbreiteter Audio- und Medienspieler der Firma Nullsoft. Winamp ist in der Lage, MP1-, MP2-, MP3-, MP4-, (Ogg)Vorbis-, AAC-, MIDI-, MOD- (sowie viele Derivate), MPC- (per Plug-in), WAV-, WMA-, WMV- (seit Version 5.12 auch mit DRM), FLAC-[1] sowie NSV-Dateien wiederzugeben, und unterstützt außerdem das Replaygain. Mit Eingabepug-ins lässt sich die Liste der unterstützten Dateiformate beliebig erweitern. Winamp lässt sich außerdem durch Skins in seinem Aussehen dem eigenen Geschmack anpassen. Durch weitere Plug-ins kann man Winamp um zusätzliche Funktionen ergänzen, z. B. Erweiterungen der Benutzeroberfläche oder das Kodieren und Konvertieren in weitere Dateiformate. Der Researcher Nicolas Joly der Firma Vupen identifizierte unlängst eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der vorliegenden Applikation. Durch die Ausnutzung der vorliegenden Schwachstelle kann unter Umständen beliebiger Code zur Ausführung gebracht werden, was zur Kompromittierung des Systems führen kann.

Expertenmeinung:

Winamp ist nach wie vor ein populärer Player für verschiedene Medienarten. Betroffene Benutzer sollten daher ein zeitnahes Update auf eine aktuelle Version anstreben.

3.10 Shemes Grabit Malicious NZB Date Denial of Service

Risiko: **problematisch**

Remote: Indirekt

Datum: 08.07.2010

scip DB: <http://www.scip.ch/?vuldb.4143>

Grabit ist ein Freeware-Client, der in erster Linie für Downloads im Usenet genutzt wird. Marc Ruef der scip AG fand eine Denial of Service-Schwachstelle in den aktuellen Versionen. Durch eine korrupte NZB-Datei kann die Anwendung zum Absturz gebracht oder ein Freeze provoziert werden. Dies lässt sich durch sehr grosse Zahlenwerte im date-Feld des jeweiligen file durchsetzen. Dadurch können laufende Downloads abgebrochen oder gar korrupt gemacht werden. Der Hersteller wurde frühzeitig über das Problem informiert und arbeitet seit geraumer Zeit an einer kompletten Neuentwicklung der Software. Diese wird voraussichtlich den Fehler nicht mehr enthalten. Als Veröffentlichungstermin ist Q3-2010 vorgesehen. Es wird empfohlen nur NZB-Dateien aus vertrauenswürdigen Quellen zu nutzen.

Expertenmeinung:

Einmal mehr zeigt auch diese Verwundbarkeit, dass Client-Applikationen grundlegende Attacken herhalten können. Das Updaten auf die aktuellste Client-Version ist entsprechend empfohlen.

3.11 Skype Client für Mac Chat Unicode Denial of Service

Risiko: **problematisch**

Remote: Ja

Datum: 21.06.2010

scip DB: <http://www.scip.ch/?vuldb.4142>

Skype ist eine in den letzten Jahren unglaublich populär gewordene freie Lösung für Internet-Telefonie. Der Skype-Client ist sehr einfach zu bedienen (ähnlich klassischen Messengern wie ICQ) und für verschiedene Plattformen erhältlich. Marc Ruef der scip AG hat eine Denial of Service-Schwachstelle im Client für Apple MacOS X gefunden. Wird über den Chat eine Nachricht empfangen, die bestimmte Unicode-Zeichen enthält, können verschiedene Funktionen der Software nicht mehr genutzt werden. So wird die korrupte Nachricht sowie alle Folgenachrichten nicht mehr dargestellt.

Ebenso ist die Chat-History für den betroffenen Benutzer nicht mehr einsehbar. Das Vorgehen zur Ausnutzung der Schwachstelle ist bekannt. Skype wurde durch ein Posting im Bug Tracking System Jira informiert und hat die Existenz der Schwachstelle bestätigt. Ein weiteres Vorgehen wurde jedoch nicht genannt. Als Workaround wird empfohlen, den Empfang von Chat-Mitteilungen nur für autorisierte Benutzer aus der eigenen Freundesliste zuzulassen.

Expertenmeinung:

Glücklicherweise lässt sich diese Schwachstelle nur in Mac-Umgebungen ausnutzen, weshalb sie - vor allem für Windows-Benutzer - nicht als akut angesehen werden muss. Wer gut und gerne Skype auf seinem Mac einsetzt, sollte jedoch dringend um eine Aktualisierung des Clients bemüht sein, sobald denn eine aktualisierte Version erscheint.

4. Statistiken Verletzbarkeiten

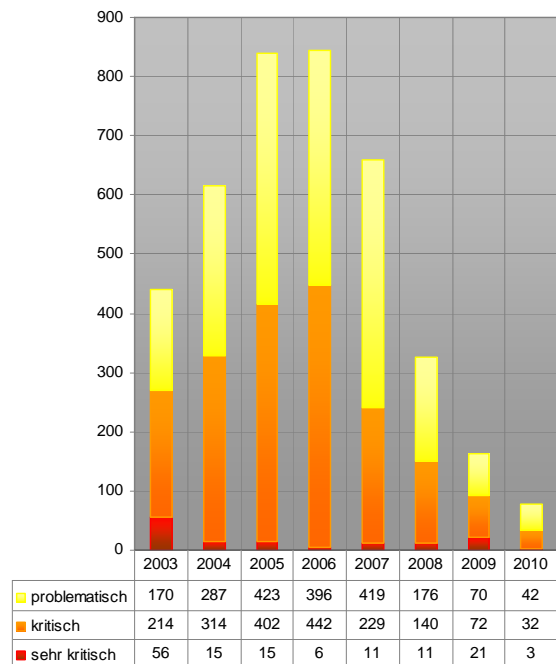
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



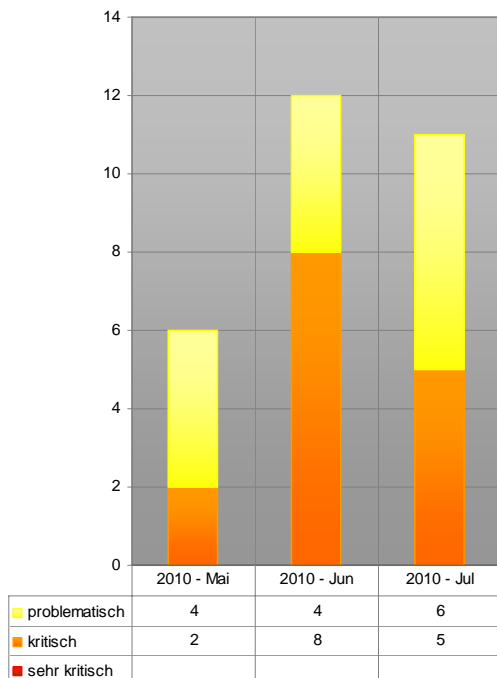
<http://www.scip.ch/?vuldb>

Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an <mailto:info@scip.ch>. Gerne nehmen wir Ihre Vorschläge entgegen.

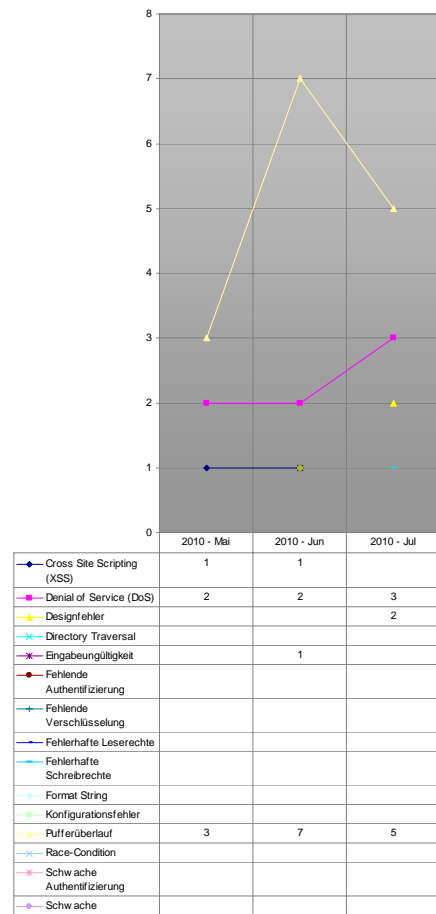
Auswertungsdatum: 19. Juli 2010



Verlauf der Anzahl Schwachstellen pro Jahr

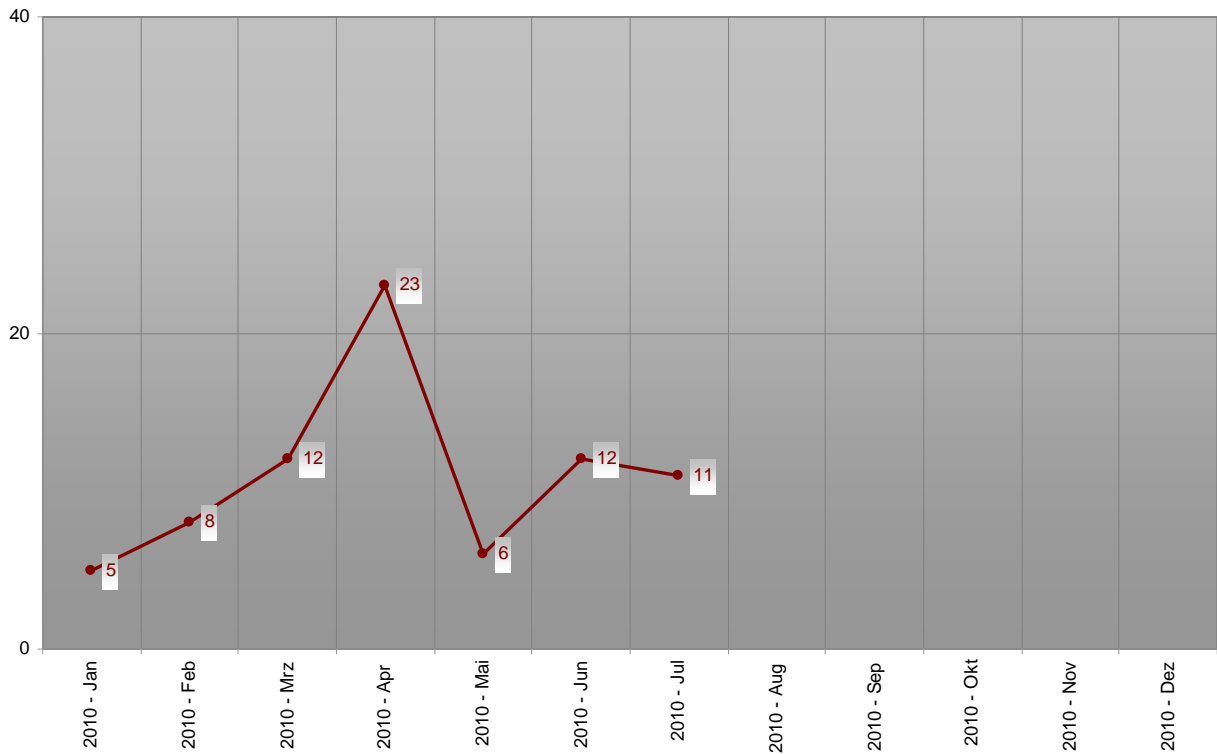


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

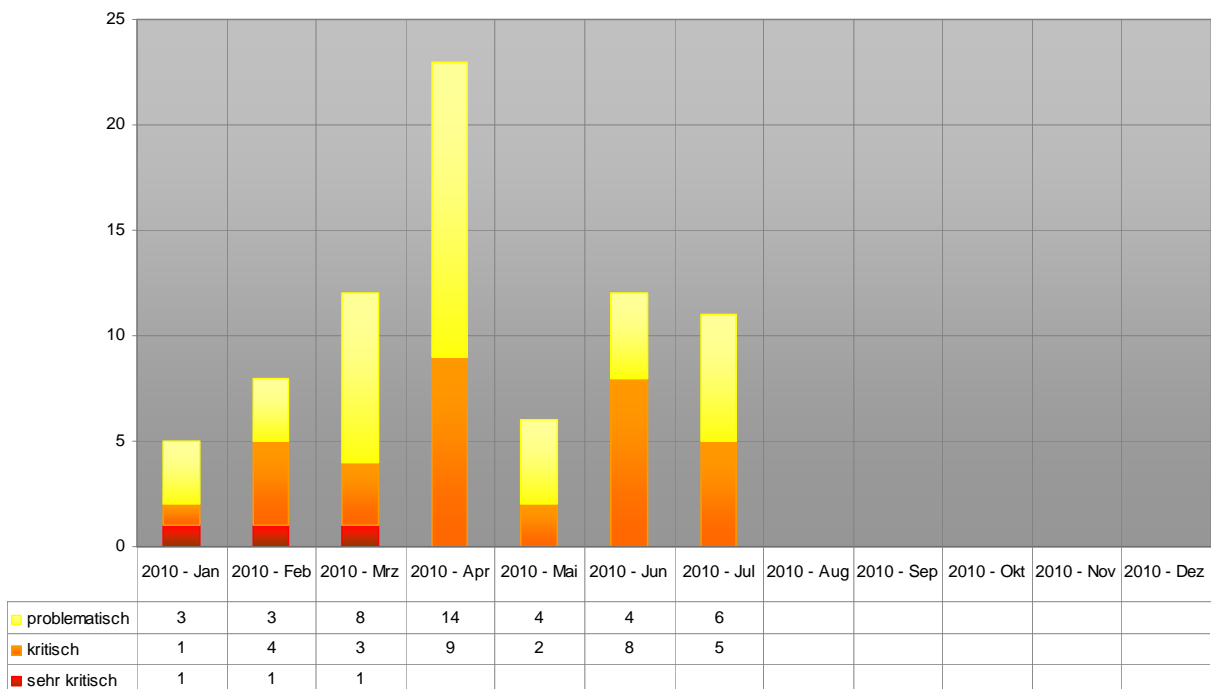


Verlauf der letzten drei Monate Schwachstelle/Kategorie

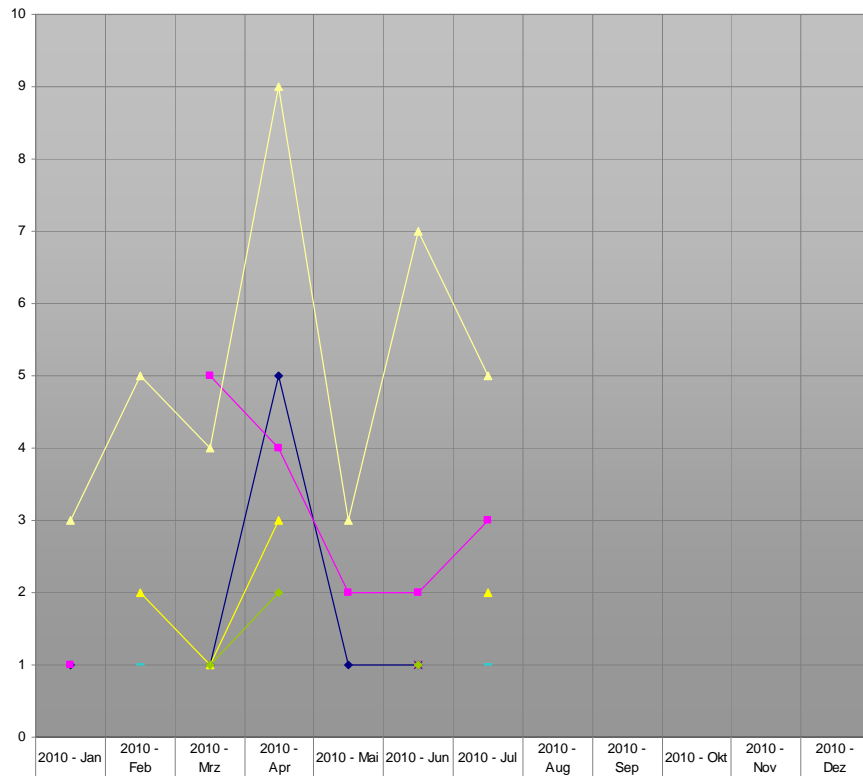
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2010



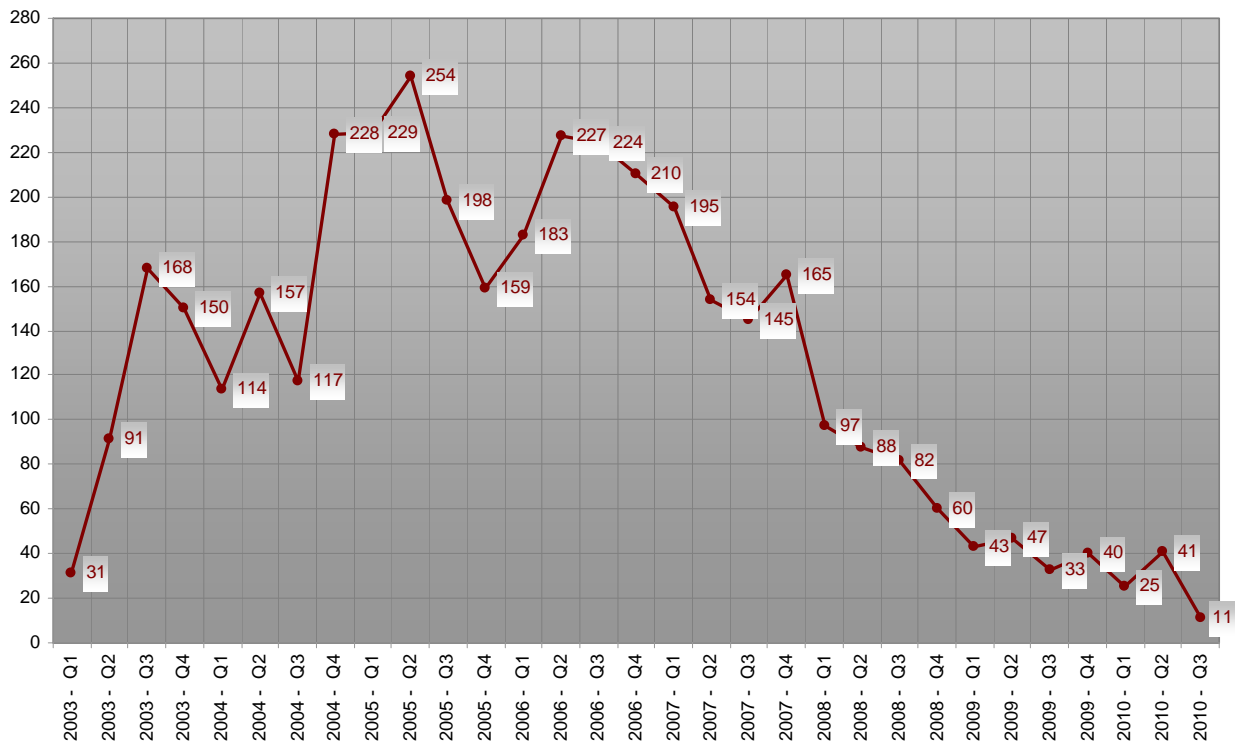
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2010



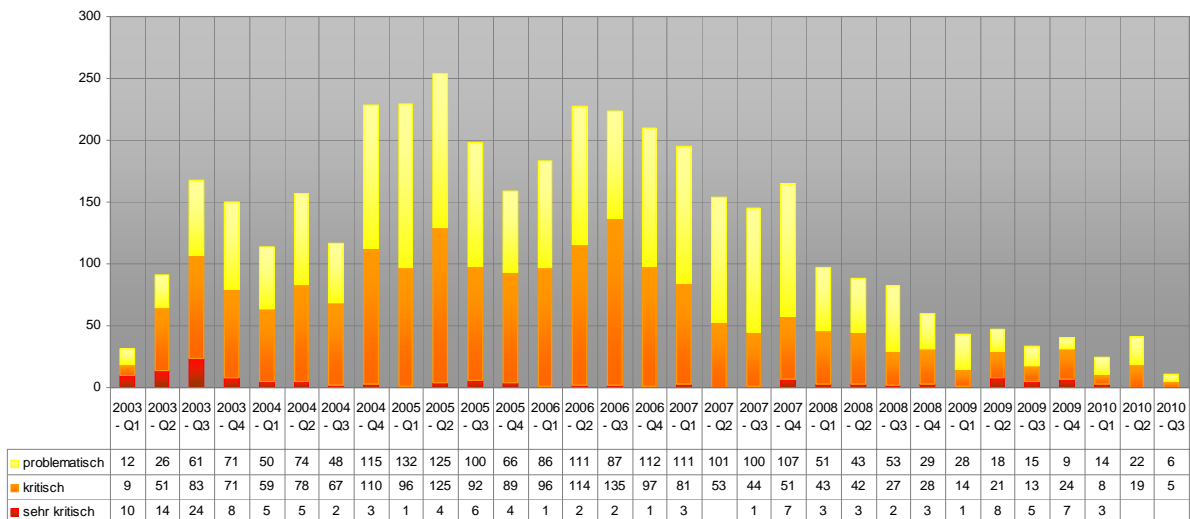
	2010 - Jan	2010 - Feb	2010 - Mrz	2010 - Apr	2010 - Mai	2010 - Jun	2010 - Jul	2010 - Aug	2010 - Sep	2010 - Okt	2010 - Nov	2010 - Dez
◆ Cross Site Scripting (XSS)	1		1	5	1	1						
◆ Denial of Service (DoS)	1		5	4	2	2	3					
◆ Designfehler		2	1	3			2					
◆ Directory Traversal												
◆ Eingabeungültigkeit						1						
◆ Fehlende Authentifizierung												
◆ Fehlende Verschlüsselung												
◆ Fehlerhafte Leserechte												
◆ Fehlerhafte Schreibrechte												
◆ Format String												
◆ Konfigurationsfehler												
◆ Pufferüberlauf	3	5	4	9	3	7	5					
◆ Race-Condition												
◆ Schwache Authentifizierung												
◆ Schwache Verschlüsselung												
◆ SQL-Injection												
◆ Symink-Schwachstelle												
◆ Umgehungs-Angriff		1					1					
◆ Unbekannt			1	2		1						

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2010

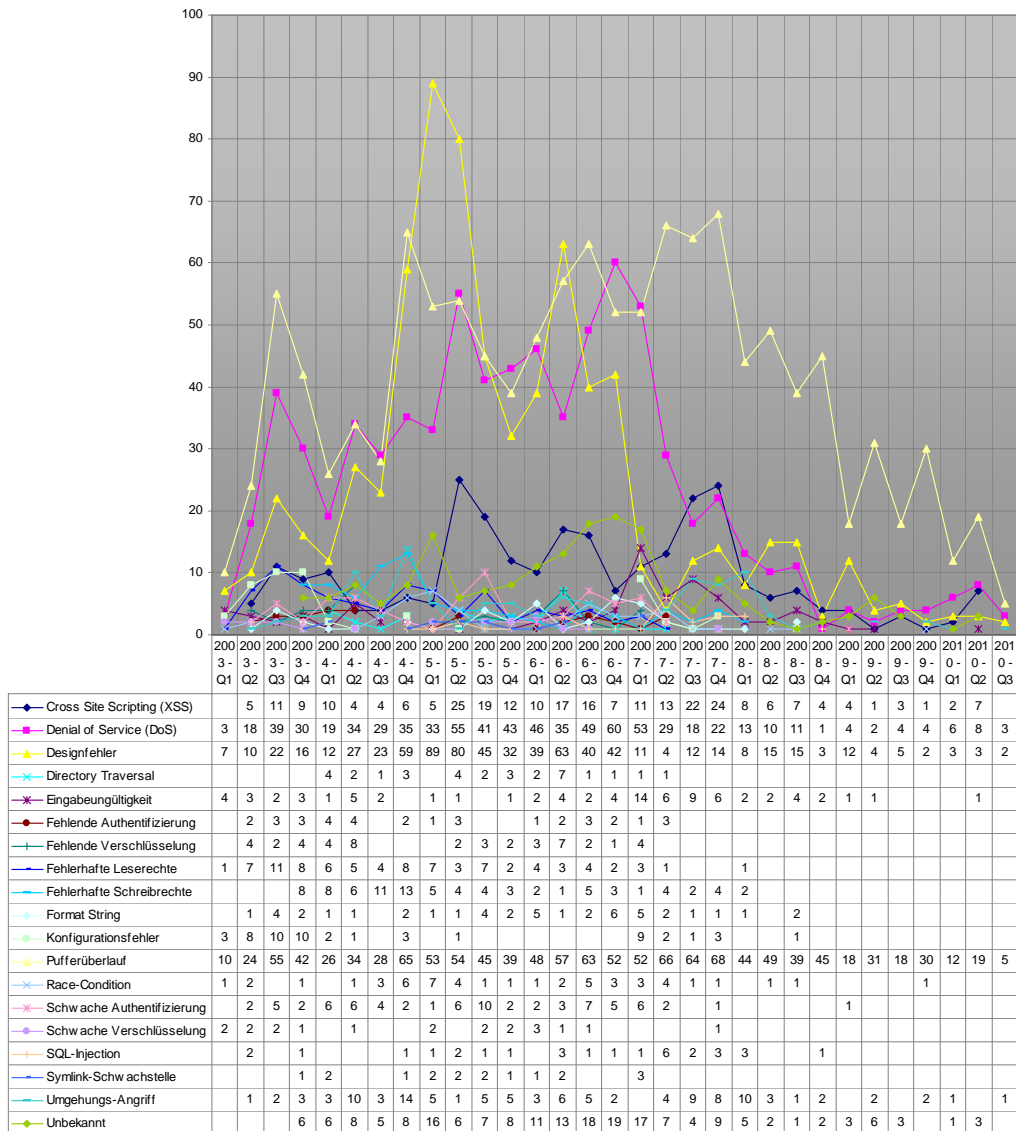
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Quartal seit 2003 Q1



Verlauf der Anzahl Schwachstellen/Schweregrad pro Quartal seit 2003 Q1



Verlauf der Anzahl Schwachstellen/Kategorie pro Quartal seit 2003 Q1

5. Labs

Auf der scip Labs Webseite (<http://www.scip.ch/?labs.archiv>) werden regelmässig Neuigkeiten und Forschungsberichte veröffentlicht.

5.1 Native Word Makro Backdoor Image Autosize Probleme

01.07.2010 Marc Ruff, maru@scip.ch

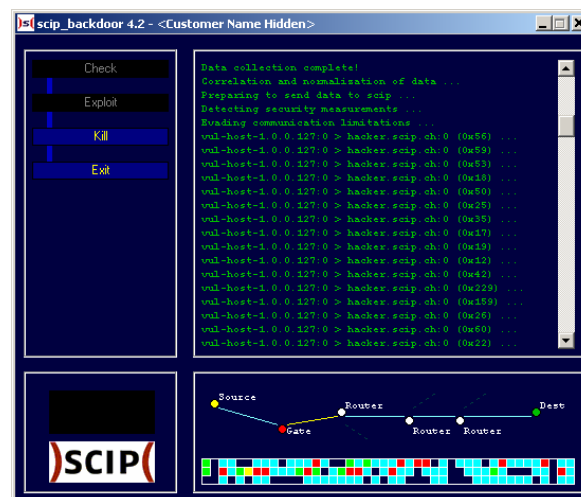
Das Durchführen von [Backdoor Tests](#) zur mehrschichtigen Prüfung von Umgebungen ist mehr denn je beliebt bei unseren Kunden. So können sie an einem konkreten Beispiel sehen, wie ein hochgradig professioneller Angreifer eine Attacke vorbereitet, diese durchführt, wie sie sich im Unternehmensnetzwerk verhält und durch die jeweiligen Stellen (Mitarbeiter, Administratoren und Incident Response Team) wahrgenommen wird.

Als Erweiterung zum klassischen Angriff mittels korrupter EXE-Datei, diese werden mittlerweile von den meisten Webproxies und Mail-Gateways gefiltert, bieten wir einen Test mit einem *nativen Word Makro Backdoor* an: Der gesamte korrupte Programmcode, der zur Fernsteuerung eines Systems genutzt wird, ist als VBA (Visual Basic for Applications) in einem harmlosen Word-Dokument (wahlweise auch in Excel, Access oder Powerpoint umsetzbar) abgelegt.

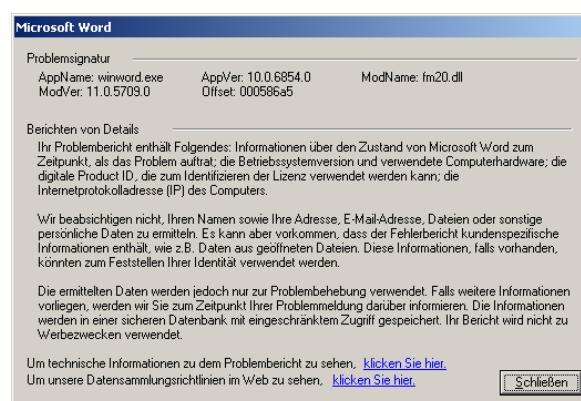
Variante	Trägerformat	Programmiersprache	Komplexität	Zuverlässigkeit
Win32	Win32 EXE	VB6 / .NET / C++	gering	mittel/hoch
VBA Dropper	MS Office	VBA + VB6 / .NET / C++	hoch	gering/mittel
VBA Native	MS Office	VBA	gering/mittel	mittel
Ajax Web Backdoor	HTML + Javascript	Javascript + PHP / ASP	mittel	hoch
Windows Mobile	CAB => EXE	.NET	mittel	mittel

Der Effekt ist für den Kunden umso grösser, desto mehr man ihn am Vorgehen des Angreifers beteiligt. So verzichten wir in der Regel darauf,

umfangreiche Stealth-Angriffe, bei denen die Aktivitäten nur mit erheblichem Aufwand erkannt werden können, durchzuführen. Stattdessen zeigen unsere Backdoors ihre Aktivitäten in einem dediziert aktivierbaren Verbose-Mode an (siehe Screenshot).



Die Word VBA Backdoor lädt sodann ein Frame, in dem die Infektion, Datensammlung und Kommunikation mit dem Angreifer illustriert wird. Dabei sind wir über ein [sonderbares Problem](#) gestolpert. Und zwar stürzt die Komponente *fm20.dll* bei Office 2000 mit einer Speichersehverletzung während des Ladens eines Images ab, wenn dessen Eigenschaft *Autosize* auf *True* gesetzt wurde.



Es verblüfft in diesem Zusammenhang unheimlich, dass mehr oder weniger problemlos mit virtuellen API-Calls und zeitkritischen Funktionen gearbeitet werden kann, während ein Autosize auf ein Image zu einem Problem mit solcher Tragweite führt. Zum Glück haben wir diese Einschränkung beim umfangreichen Unit-Test [frühzeitig bemerkt](#) und entsprechende Massnahmen ergreifen können. Es gibt schliesslich nichts Schlimmeres, weder wenn korrupter Programmcode in einem Realworld-Test mit einer aufdringlichen Fehlermeldung abstürzt.

In unserem Kundenumfeld ist in den letzten 2 Jahren der Trend [zu beobachten](#), erweiterte Makros in Office-Dokumenten wieder zuzulassen. Die Sicherheitseinstellungen in den Applikationen werden oftmals auf Mittel oder gar Gering gesetzt und die Sicherheit einzig und allein auf Antiviren-Mechanismen abgestützt. Wir raten vollumfänglich von diesem Ansatz ab, da er die Risiken von durchdachter Malware auf der Basis von Makros *nicht vertretbar* adressieren kann (dies betrifft ebenfalls [LotusScript](#)). Durch verschiedene Evasion-Techniken, die wir erfolgreich weiterentwickelt und eingesetzt haben, lassen sich ein Grossteil der etablierten Technologien und Ansätze umgehen.

6. Bilderrätsel



GESUCHTE BEGRIFFE		
11 (english)	10 (english)	10 (english)

LÖSUNGSWORT

scip monthly Security Summary 19.07.2010

Wettbewerb

Mailen Sie uns das Lösungswort an die Adresse <mailto:info@scip.ch> inklusive Ihren Kontakt-Koordinaten.

Das Los entscheidet über die Vergabe des Preises. Teilnahmeberechtigt sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.08.2010**.

Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises.

Gewinnen Sie ein Exemplar des Buches „Die Kunst des Penetration Testing“ von Marc Ruef. Dem meistverkauften deutschsprachigen Penetration Testing Fachbuch auf dem Markt.



<http://www.computec.ch/mruef/?s=dkdpt>

911 Buchseiten, ISBN 3-936546-49-5

7. Impressum

Herausgeber:



scip AG
Badenerstrasse 551
CH-8048 Zürich
T +41 44 404 13 13
<mailto:info@scip.ch>
<http://www.scip.ch>

Zuständige Person:



Marc Ruff
Security Consultant
T +41 44 404 13 13
<mailto:maru@scip.ch>

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich Information Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, Trend-Micro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserungen möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summarys finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)