

The World of Warcraft Warden program viewed under spyware aspects

Patrick M. Kolla

24. März 2006

Inhaltsverzeichnis

1. Einleitung	2
1.1. Aktualität	3
2. Analyse	3
2.1. Lizenzbestimmungen	3
2.1.1. Arbeitsspeicher	3
2.1.2. Geladene Module	4
2.1.3. Laufende Prozesse	4
2.1.4. Zwischenergebnis	5
2.2. Online-Persönlichkeitsrecht-Grundsätze	5
2.2.1. Blizzard Datenschutzhinweise	5
2.2.2. Anfrage per E-Mail an zuständige Adresse	5
2.2.3. Anfrage per Telefon unter zuständiger Nummer	6
2.2.4. Anfrage per Kundendienst-Kontaktformular	6
2.2.5. Anfrage per Support-Forum	7
2.2.6. Anfrage per E-Mail an Account Administration Team	7
2.2.7. Zwischenergebnis	7
3. Dateianalyse	8
3.1. PE-Ansicht	8
3.1.1. Entwicklung	9
3.1.2. Zwischenergebnis	9
4. Zusammenfassung	10

A. API-Calls	11
A.1. Statisch verlinkte Funktionen	11
A.1.1. kernel32.dll	12
A.1.2. user32.dll	13
A.1.3. advapi32.dll	13
A.2. Dynamisch verlinkte Funktionen	13
A.2.1. kernel32.dll	13
A.2.2. user32.dll	13
A.2.3. mscoree.dll	13
A.3. Exportierte Funktionen	13
B. Quellen und Verweise	14
C. Ergänzende Texte	14
C.1. Kommunikation an und von Blizzard	14
C.1.1. Forenbeitrag	14
C.1.2. Formbrief von Granite, Account Administration Team	15



Copyright

Dieses Dokument wurde von der Safer Networking Ltd. für die eigene Wissensdatenbank sowie zur rein informativen Nutzung ihrer Kunden erstellt. Das Copyright liegt ausschließlich bei der Safer Networking Ltd., kommerzielle Nutzung dieses Dokumentes durch Dritte, ist ausdrücklich untersagt und kann nur in Ausnahmefällen schriftlich genehmigt werden. Als Ausnahme gilt die Presse, solange die Quelle unmissverständlich angegeben wird.

1. Einleitung

Dieses Dokument setzt sich näher auseinander mit Kritiken an *Warden*, den Anti-Cheat-Bemühungen *Blizzards* im MMORPG *World of Warcraft*. Sämtliche Untersuchungen basieren auf einer deutschen Version von *World of Warcraft* mit installiertem Patch 1.9.4.

1.1. Aktualität

Dieser Fall ist noch nicht endgültig abgeschlossen; die in diesem Dokument enthaltenen Informationen sind daher nur als vorläufige Erkenntnisse anzusehen. Wir werden uns bemühen, dieses Dokument auf einen endgültigen und besser ausformulierten Stand zu bringen, sobald ein Ende absehbar ist.

2. Analyse

2.1. Lizenzbestimmungen

In diesem Abschnitt werde ich auf die den Warden betreffenden Abschnitte in den Lizenzbestimmungen eingehen.

2.1.1. Arbeitsspeicher

Um den Bemühungen der Einzelpersonen, die bereit sind die EULA und/oder die TOU zu verletzen, entgegen zu wirken, nutzt Blizzard Entertainment eine ‘Anti-Cheating-Software’, die als Teil von World of Warcraft läuft. Diese ‘Anti-Cheating-Software’ scannt in eingeschränktem Umfang:

(i) den Arbeitsspeicher (Random Access Memory, ‘RAM’), der mit dem World of Warcraft Programm belegt ist, um zu prüfen, ob das World of Warcraft Programm unter Verstoß gegen die World of Warcraft Nutzungsbestimmungen verändert oder ‘gehackt’ wurde; [...]

Welcher RAM gescannt wird, ist hier klar eingeschränkt - der von WoW sowieso belegte RAM. Wenn ein Programm gestartet wird, wird dieses Programm in den Arbeitsspeicher geladen¹ und bekommt unter Umständen einen weiteren Bereich im Arbeitsspeicher zugewiesen², um darin eigene Daten zu verwalten. Dass ein Programm Zugriffsrechte³, zumindest für Lese-Operationen, auf beide Bereiche hat, ist nur logisch; und der lesende Zugriff auf den eigenen Arbeitsspeicher keinerlei Gefährdung einer Privatsphäre an sich. Der Bereich für Daten kann bzw. sollte von regulären Programmen auch nicht von außen mit Daten gefüllt werden können (Sicherheitsaspekt *Protected Memory*, der ab Windows NT gegeben ist), so dass auf diesem Wege keine ungewollten Daten an Blizzard gehen. Nimmt man den Text von Blizzard aber wörtlich, betrifft dies sogar nur den vom Programm selber belegten Speicher, als nur das Code-Segment. Auch in dieses kann reguläre Software von außen nichts hineinschreiben - dies geht nur über die so genannte *Code Injection*, eine Methode, die zum überwiegenden Teil von diversen Cheats verwendet wird. Reguläre Anwendungen zur Datenverarbeitung nutzen diese so gut wie nie, lediglich in ein paar Sicherheits-Anwendungen ist sie zu finden. Dass auf diese Weise persönliche Daten in den vom Warden geprüften Speicherbereich kommen, ist daher so gut wie ausgeschlossen, lediglich Cheats können wirksam erkannt werden.

¹Dieser Teil des Speichers wird i.d.R. Code-Segment genannt.

²Als Daten-Segment bezeichnet.

³`kernel32.dll:ReadProcessMemory`

Es bleibt die (für die Sicherheit aber irrelevante) Frage an Blizzard, ob nur Code- oder auch Daten-Segmente geprüft werden.

2.1.2. Geladene Module

[...] (ii) den World of Warcraft ‘Prozess’, um festzustellen, ob ein nicht-autorisiertes Programm eines Drittanbieters oder Computercode mit dem World of Warcraft Prozess verbunden wurde und [...]

Auch diese Überprüfung ist relativ normal und nur auf *WoW* bezogen. Als vergleichendes Beispiel könnte man erwähnen, dass der Internet Explorer verwaltet, welche BHOs (Browser Helper Objects - z.B. Google Toolbar) installiert wurden. Diese laufen als flexible Module in den Prozess eingebunden; derartige für die Verwendung des Prozesses gedachte Module lassen sich von innen und von außen⁴, einsehen⁵. Per Code Injection⁶ ist es möglich, auch ungewollte Module nachträglich in Prozesse einzubinden, was von Blizzard hier geprüft wird. Da jedes Programm nun Zugriff auf die Module hat, die es geladen hat⁷, ist auch hier nichts schlimmes zu erkennen. Zugriff über die Module hinaus auf externe Daten ist mit der hier beschriebenen Technologie ebenfalls nicht möglich.

2.1.3. Laufende Prozesse

[...] (iii) die Windows Prozessliste, um festzustellen, ob ein Cheat- oder Hack-Programm gegenwärtig unter Verstoß gegen die World of Warcraft Nutzungsbestimmungen geöffnet ist.

Die Prozess-Liste selber enthält keine persönlichen Daten, lediglich Namen von Programmen zusammen mit lediglich für den Betrieb wichtigen Informationen (Anzahl der offenen Dateien - nicht deren Inhalte, Priorität, Name des Programms auf der Platte - nicht dessen Inhalt, etc.). Unter Windows NT und neueren Betriebssystemen dieser Reihe⁸ kann jeder Benutzer mit entsprechenden Rechten diese selber einsehen, indem er Strg+Alt+Entfernen drückt und sich die Prozessliste im Task Manager anzeigen lässt.

Wer sich die Liste der statisch importierten Funktionen in *scan.dll* ansieht, wird die Funktionen finden, die für obige relativ harmlose Scans notwendig sind⁹, jedoch noch nicht einmal Funktionen die i.d.R. dafür genutzt werden, Dateilisten zu erstellen. Ebenfalls kann *Warden*, genauer gesagt die Datei *scan.dll*, einzelne Prozesse beenden¹⁰.

⁴Bei ausreichenden Rechten *advapi32.dll:LookupPrivilegeValueA*, *advapi32.dll:AdjustTokenPrivileges*, unter anderem wird *SeDebugPrivilege* gesetzt.

⁵*kernel32.dll:GetModuleHandleA*, *kernel32.dll:GetModuleFileNameA*

⁶Näher beschrieben in Abschnitt 2.1.1.

⁷Sie werden eben zur Nutzung durch den Prozess geladen.

⁸also auch Windows 2000, XP und 2003

⁹*kernel32.dll:Process32First*, *kernel32.dll:Process32Next*, *kernel32.dll:CreateToolhelp32Snapshot*

¹⁰*kernel32.dll:TerminateProcess*

Leider nicht explizit erwähnt wird das Überprüfen der Fenstertitel¹¹. Fenstertitel beinhalten sehr eingeschränkte Informationen¹², hier kommt es stark darauf an, ob diese an Blizzard übermittelt oder nur lokal gegen eine statische Liste verglichen werden.

2.1.4. Zwischenergebnis

[...] Darüber hinaus wird darauf hingewiesen, dass Blizzard derzeit außer der soeben dargestellten Scanaktivitäten keine anderen Scans des von Ihnen zum Spielen von World of Warcraft genutzten Computers durchführt.

Vergleicht man die technischen Gegebenheiten ohne *Reverse Engineering* mit den Lizenzbestimmungen, sind diese deckungsgleich und beinhalten keine Methoden, die definitiv unerlaubt in die Privatsphäre des Benutzers eindringen würden.

Schade bleibt hier nur, dass Blizzard zu keiner Stellungnahme bereit ist und daher die im vorigen Abschnitt beschriebenen Zweifel nicht ausräumen konnte. Die untersuchten Dateien enthielten nicht explizit Funktionen, wie sie zum Austausch von Daten mit dem Internet in der Regel verwendet werden; da die Warden-Funktionalität jedoch von anderen Programmen¹³ aufgerufen wird, kann eine Übermittlung durchaus auch dort stattfinden, womit dieser Punkt offen bleibt.

2.2. Online-Persönlichkeitsrecht-Grundsätze

2.2.1. Blizzard Datenschutzhinweise

Blizzard bietet selber die nach Datenschutzgesetzen vorgeschriebene Auskunft über gespeicherte Daten mit folgendem Text an¹⁴:

Wenn Sie aus irgendeinem Grund genau wissen möchten, in welcher Weise wir Ihre persönlichen Daten verwenden, oder wenn Sie Informationen korrigieren oder uns die weitere Verwendung Ihrer persönlichen Daten untersagen möchten, setzen Sie sich bitte mit Blizzard unter folgender Adresse in Verbindung: Blizzard Entertainment Europe, TSA 60 001, 78143 Vélizy Villacoublay Cedex France. Sie können uns auch telefonisch unter der Rufnummer 0033 1 30 67 90 00 oder per E-Mail webmaster-de@blizzard.com benachrichtigen.

2.2.2. Anfrage per E-Mail an zuständige Adresse

Um die Ernsthaftigkeit, mit der Blizzard mit der Privatsphäre seiner Kunden umgeht, weiter zu ergründen, bietet es sich an, dass ein WoW-Spieler auf dem genannten Weg - per E-Mail, um eine gegebenenfalls eindeutig reproduzierbare Antwort zu erhalten - Einsicht

¹¹`user32.dll:EnumWindows, user32.dll:GetWindowTextA`

¹²Ein Fenstertitel namens *Winword: Kündigungsbrief an Firma.doc* wäre ein Extrembeispiel.

¹³etwa dem Launcher und dem Hauptprogramm

¹⁴Stand der Datenschutzvereinbarung bzw. letzte Aktualisierung: 9. August 2004

in die über ihn gespeicherten Daten verlangt. Der für diese Anfrage verwendete Text lautete¹⁵:

E-Mail an Blizzard
Von: wowspieler@example.com¹⁶
An: webmaster-de@blizzard.com
Betreff: Auskunft über gespeicherte Daten zu WoW-Account

Wie auf ihrer den Datenschutz betreffenden [Webseite](#) beschrieben, wende ich mich hiermit an sie, um Einsicht in die über mich gespeicherten Daten zu erhalten. Die zu meinem *World of Warcraft*-Account mit dem Namen *Unleserlich* gehörenden Informationen schicken sie bitte an die Absenderadresse dieser E-Mail, *wowspieler@example.com*. Für Rückfragen zu dieser Anfrage stehe ich jederzeit unter dieser E-Mail-Adresse oder unter der mit dem Account verknüpften Telefonnummer zur Verfügung, und bitte um Beantwortung innerhalb einer Woche (5 Werktagen) bzw. gegebenenfalls Mitteilung, wann eine ausführliche Auskunft ca. erfolgen wird.

Im Rahmen dieser Untersuchung ist dies zweimal, mit leicht abgewandeltem Text von unterschiedlichen Adressen¹⁷ aus mit jeweils einer siebentägigen Frist geschehen, ohne dass Blizzard geantwortet hätte.

2.2.3. Anfrage per Telefon unter zuständiger Nummer

Am 20. März riefen wir dann die von Blizzard genannte Telefonnummer¹⁸ an. Eine nette französische Dame am Telefon konnte zwar keine Durchwahl mitteilen¹⁹, und ebenfalls keine direkte E-Mail-Adresse²⁰, war jedoch sehr bemüht, jemanden ans Telefon zu bekommen, und nach einer Viertelstunde vergeblicher Bemühungen so freundlich, selber eine E-Mail an eine verantwortliche Person mit der Bitte um Kontaktaufnahme zu schreiben.

Auch auf diesem Weg war knapp fünf Tage später - trotz Hinweis auf Dringlichkeit - noch kein Kontakt aufgenommen worden.

2.2.4. Anfrage per Kundendienst-Kontaktformular

Da Blizzard alle drei Wege (E-Mail, Telefon und Post) als Alternativen angibt, wären wir sicherlich nicht verpflichtet gewesen, mehr als einen Weg zu probieren; um aber wenigstens eine Stellungnahme zu erhalten, haben wir uns noch für einen dritten Weg

¹⁵Persönliche Informationen wurden hier unkenntlich gemacht

¹⁶Unkenntlich gemacht, Original-Email enthält eine Email-Adresse, die zu einem später erwähnten gültigen Accountnamen gehört.

¹⁷Um Empfangsprobleme durch Spamfilter o.ä. auszuschließen, bei der Adresse, die nicht mit dem Account verknüpft war, wurde auf diesen Umstand zusätzlich hingewiesen.

¹⁸0033 1 30 67 90 00

¹⁹Interne Nummer würden sich von externen unterscheiden.

²⁰Die verantwortlichen haben nur persönliche E-Mail-Adressen.

entschieden. Der Rechnungssupport, für Fälle Rechnungen und Account betreffend, ist bzw. sollte auch über ein Web-Formular erreichbar sein.

Dieser ist jedoch scheinbar nicht erreichbar; bei dem Versuch, die Mitteilung abzusenden, erschien lediglich eine Fehlermeldung. Es fehlte jegliche Fehlermeldung außer dem Hinweis, die Eingabefelder alle nochmals zu überprüfen. Diverse E-Mail-Adressen, gekürzte Texte²¹ und verschiedene Browser führten ebenfalls zu keinem Ergebnis.

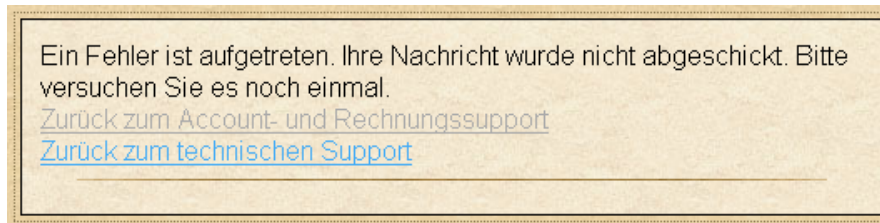


Abbildung 1: Der Kundendienst ist per Kontaktformular nicht erreichbar

2.2.5. Anfrage per Support-Forum

Als vierte Möglichkeit, Blizzard zu kontaktieren, bleibt noch das offizielle Support-Forum; in diesem Fall im deutschen *Vorschläge*-Unterforum. Am 22. März 2006 um 13:57 Uhr²² haben wir einen Beitrag mit dem Betreff **Blizzard & das Bundesdatenschutzgesetz**²³ mit der Topic-ID 139147 online gestellt. Reagiert haben darauf lediglich betroffene Spieler, aber wiederum nicht Blizzard.

2.2.6. Anfrage per E-Mail an Account Administration Team

Mit der Bitte um Kontaktherstellung zu Blizzards Rechtsabteilung habe ich mich ebenfalls am 23. März um 11:17 Uhr an das **Account Administration Team** gewandt. Bereits um 17:28 Uhr hat eine Person namens *Granite* geantwortet - jedoch leider nur einen Formbrief, der ganz lapidar auf die bekannte und von Blizzard nicht befolgte eigene **Datenschutzvereinbarung** hinweist²⁴. Eine erneute Anfrage lieferte, immerhin nach nur wenigen Stunden Geschäftszeit, wiederum nur einen Hinweis auf die bereits aus der Datenschutzvereinbarung bekannten Adressen.

2.2.7. Zwischenergebnis

Die unbeantworteten E-Mails lassen zwar keinen Rückschluss auf widerrechtliche Datensammlung zu, dennoch zeigen sie, dass Blizzard die Datenschutzgesetze zumindest im

²¹Die selbstverständlich keine Anführungszeichen etc. beinhalten, da uns von vorherigen Kontaktversuchen bekannt war, dass Blizzard Probleme mit korrekter MySQL-Programmierung hat.

²²Die Forenuhr zeigt eine andere Zeitzone und geht zudem scheinbar falsch; sie zeigt 3/22/2006 4:06:16 PM PST

²³Am gleichen Tag korrigiert auf *Einhaltung des Bundesdatenschutzgesetzes*, da Blizzard droht, Beiträge mit *Blizzard* im Namen nicht zu berücksichtigen.

²⁴Eine Kopie der Email ist in Abschnitt **C.1.2** auf Seite **15** zu finden.



Abbildung 2: Ein frischer Beitrag im Vorschläge-Unterforum

elektronisch-kommunikativen Umgang mit seinen Kunden nicht sonderlich zu beachten scheint. Ob von einem Kunden erwartet werden kann, eine Nummer in Frankreich anzurufen und dort englisch oder französisch zu sprechen, mag ebenfalls bezweifelt werden können, dennoch machte der Anruf einen besseren Eindruck - immerhin kümmerte sich jemand gründlich, wenn auch leider erfolglos, um das Problem. Nach etlichen Versuchen über fünf Kontaktmöglichkeiten bleibt aber trotzdem nur noch die Einschaltung des Landesdatenschutzbeauftragten. Nach einem Telefonat mit Herrn Kaminski, Mitarbeiter der Landesbeauftragten für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen, ist dieses Dokument nun unterwegs zu deren Poststelle.

3. Dateianalyse

3.1. PE-Ansicht

Section	VirtSize	VirtAddr	PhysSize	PhysAddr	Flags	CRC32
.text	00005FB4	00001000	00006000	00001000	60000020	7324BB0B
.rdata	00001BB5	00007000	00002000	00007000	40000040	865E17DF
.data	0000113C	00009000	00001000	00009000	C0000040	6786BCBA
.rsrc	00000360	0000B000	00001000	0000A000	40000040	03F18CA0
.reloc	00000D32	0000C000	00001000	0000B000	42000040	964BD4BC

Abbildung 3: Eine Übersicht der PE-Segmente in scan.dll

PE steht für *Portable Executable* und bezeichnet ein Format, nach dem alle ausführba-

ren Windows-Dateien (neben EXE auch DLL, SCR und einige andere) aufgebaut sind. In dieser Struktur lassen sich Informationen wie etwa Listen der benutzten externen Funktionen²⁵ sehr einfach auffinden. Auffällig ist hier erst einmal, dass der PE-Kopf anzeigt, dass das Code-Segment an der Adresse 0x1000 zu finden wäre - dort ist laut PE-Segment-Tabelle aber ein Segment namens *.text*.

Linker version (major)	07
Linker version (minor)	0A
Size of code	00006000
Size of initialized data	00006000
Size of uninitialized data	00000000
Address of entry point	0000240E
Base of code	00001000
Base of data	00007000

Abbildung 4: Ein Ausschnitt des PE-Headers, der auf das Code-Segment zeigt

Dies dürfte einen simplen Versuch, das Verständnis der Datei zu erschweren, darstellen. Weitere ernsthafte Verschleierungsversuche, wie etwa das sehr übliche UPX, sind aber nicht vorhanden.

3.1.1. Entwicklung

Die Datei wurde mit Microsoft Visual C++ erstellt, was angesichts der weiten Verbreitung von C++ nicht weiter verwunderlich ist. Lediglich die Verwendung eines Microsoft-Produktes scheint bei einem plattformübergreifenden Produkt merkwürdig; da diese Datei aber nicht das eigentliche Produkt darstellt und der Compiler keinen Einfluß auf das Thema dieses Artikels hat, sei dies nur am Rande bemerkt.

Erstellt wurde die *scan.dll* weiterhin im Ordner *C:\Projects\Tools\Launcher\Win32\Scan*, was den Schluß nahelegt, dass diese Datei eng mit dem *Launcher* verknüpft ist. Dieser lädt die *scan.dll* jedoch zumindest nicht dauerhaft ein.

Von einem schlechten Stil zeugt die Verwendung der Funktion `kernel32.dll:SetHandleCount`, die unter 32-bit Windows keinerlei Funktion mehr hat und lediglich aus Rückwärtskompatibilität zu 16-bit Windows²⁶ überhaupt noch existiert.

3.1.2. Zwischenergebnis

Die Dateianalyse bestätigt noch einmal die bereits in Abschnitt 2.1 getätigten Vergleiche mit den Lizenzbestimmungen. Es gibt keine offensichtlichen Verstöße, die ohne *Reverse Engineering*²⁷ festgestellt werden konnten.

²⁵Siehe auch Abschnitte A.1 und A.2.

²⁶wie etwa Windows 3.1, 3.11, Windows for Workgroups

²⁷Reverse Engineering bezeichnet das Umwandeln des Programmcodes in menschenlesbare Form, und schrittweise Abarbeitung dieser zum Verständnis der Funktion.

4. Zusammenfassung

Abschließend bleibt zu sagen, dass die Funktionalität zur Überprüfung nach installierten, den Nutzungsbedingungen widersprechenden Cheats ziemlich genau dem entspricht, was Blizzard auch selber für jeden Benutzer sichtbar²⁸ angibt. Lediglich die Möglichkeit, andere Programme zu beenden - die allerdings mehr oder weniger selbstverständlich ist - wurde verschwiegen und bei der Erwähnung der Überprüfung laufender Prozesse die - trotzdem allseits bekannte - Überprüfung von Fenstertiteln nicht ausdrücklich erwähnt²⁹.

Blizzard gibt weiterhin - obwohl rechtlich vorgeschrieben und von Blizzard selber angekündigt - *keine* Auskunft über gespeicherte Daten, was jeden Datenschützer aufhorchen lassen sollte. Nach vergeblichen Kontaktversuchen auf vier verschiedenen Wegen kann Blizzard sich auch kaum noch auf schlechte Mitarbeiterschulung oder Nachlässigkeit berufen. Auch wenn dem *Warden* in diesem Fall keine die Privatsphäre verletzenden Aktivitäten vorgeworfen werden konnten, muss doch davon ausgegangen werden, dass Blizzard seine fehlenden Skrupel im Datenschutz jederzeit auch aktiv einsetzen und auch im *Warden* geltendes Recht verletzen würde, sollte es sich daraus einen Vorteil versprechen.

Für eine endgültige Bewertung bleibt nun auf die Hilfe der Landesbeauftragten für Datenschutz und Informationsfreiheit zu warten.

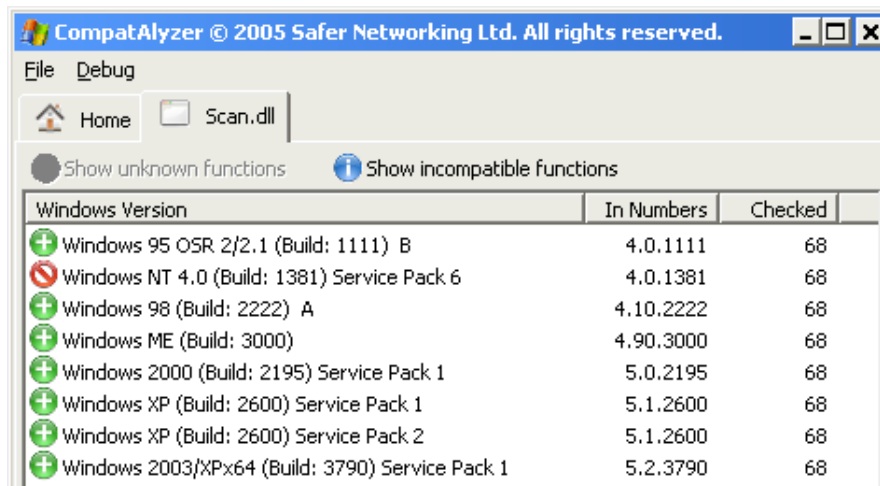
²⁸Zuletzt deutlich sichtbar nach Installation des letzten Patches

²⁹Siehe Bedenken in Abschnitt [2.1.2](#).

A. API-Calls

A.1. Statisch verlinkte Funktionen

Statisch verlinkte Funktionen sind solche, die ein Programm zwingend benötigt, um ausgeführt werden zu können. Auch eine DLL zählt hierbei als Programm.



Windows Version	In Numbers	Checked
Windows 95 OSR 2/2.1 (Build: 1111) B	4.0.1111	68
Windows NT 4.0 (Build: 1381) Service Pack 6	4.0.1381	68
Windows 98 (Build: 2222) A	4.10.2222	68
Windows ME (Build: 3000)	4.90.3000	68
Windows 2000 (Build: 2195) Service Pack 1	5.0.2195	68
Windows XP (Build: 2600) Service Pack 1	5.1.2600	68
Windows XP (Build: 2600) Service Pack 2	5.1.2600	68
Windows 2003/XPx64 (Build: 3790) Service Pack 1	5.2.3790	68

Abbildung 5: Eine Kompatibilitätsanalyse der statisch verlinkten Funktionen in scan.dll

Es folgt eine Liste der statisch verlinkten Funktionen, an wichtigen Stellen verlinkt auf die entsprechenden Webseiten im Microsoft Developer Network.

A.1.1. kernel32.dll

- CreateToolhelp32Snapshot
- ReadProcessMemory
- OpenProcess
- Process32First
- Process32Next
- CloseHandle
- GetVersionExA
- GetCurrentProcess
- ExitProcess
- GetCurrentThreadId
- GetCommandLineA
- QueryPerformanceCounter
- GetTickCount
- GetCurrentProcessId
- GetSystemTimeAsFileTime
- GetModuleFileNameA
- GetProcAddress
- GetModuleHandleA
- TerminateProcess
- TlsAlloc
- SetLastError
- GetLastError
- TlsFree
- TlsSetValue
- TlsGetValue
- HeapFree
- HeapAlloc
- SetHandleCount³⁰
- GetStdHandle
- GetFileType
- GetStartupInfoA
- DeleteCriticalSection
- FreeEnvironmentStringsA
- GetEnvironmentStrings
- FreeEnvironmentStringsW
- WideCharToMultiByte
- GetEnvironmentStringsW
- HeapDestroy
- HeapCreate
- VirtualFree
- UnhandledExceptionFilter
- WriteFile
- LoadLibraryA
- RtlUnwind
- InterlockedExchange
- VirtualQuery
- LeaveCriticalSection
- EnterCriticalSection
- GetACP
- GetOEMCP
- GetCPInfo

³⁰Diese Funktion ist in 32-bit-Windows nicht mehr benötigt und nur noch aus Rückwärtskompatibilitätsgründen zu 16-bit vorhanden.

- VirtualAlloc
- HeapReAlloc
- InitializeCriticalSection
- HeapSize
- GetLocaleInfoA
- GetStringTypeA
- MultiByteToWideChar
- GetStringTypeW
- LCMapStringA
- LCMapStringW
- VirtualProtect
- GetSystemInfo

A.1.2. user32.dll

- EnumWindows
- GetWindowTextA

A.1.3. advapi32.dll

- OpenProcessToken
- LookupPrivilegeValueA
- AdjustTokenPrivileges

A.2. Dynamisch verlinkte Funktionen

Da die *scan.dll* auf dynamisch nachgeladene Funktionen zugreifen kann³¹, müssen wir uns die derart benutzten Funktionen auch noch ansehen.

³¹kernel32.dll:LoadLibrary, GetProcAddress

kernel32.dll:-

A.2.1. kernel32.dll

- InitializeCriticalSectionAndSpinCount

A.2.2. user32.dll

- GetActiveWindow
- GetLastActivePopup
- GetProcessWindowStation
- GetUserObjectInformationA
- MessageBoxA

A.2.3. mscoree.dll

- CorExitProcess

A.3. Exportierte Funktionen

Die Datei *scan.dll* exportiert nur eine einzige, nur per Nummer identifizierbare³² Funktion.

³²i.d.R. haben Funktionen in DLLs Namen, die deren Funktion beschreiben, siehe Liste der importierten bzw. verlinkten Funktionen

B. Quellen und Verweise

- Bundesministerium der Justiz: Bundesdatenschutzgesetz
http://bundesrecht.juris.de/bdsg_1990/
- Blizzard: Webseite
<http://www.blizzard.de/>
- Blizzard: World of Warcraft
<http://www.wow-europe.com/de/>
- Blizzard: Rechtliches
<http://www.wow-europe.com/de/legal/>
- Blizzard: Datenschutzvereinbarung
<http://www.blizzard.de/privacy.shtml>
- Blizzard: Kundendienst-Kontaktformular
<http://www.wow-europe.com/support/webform/billingDefault.html?lan=de>
- Blizzard: Email des Verantwortlichen für Datenschutz
webmaster-de@blizzard.com
- Blizzard: Email der Account-Abteilung
WoWAccountReviewEU@blizzard.com
- Safer Networking: Forenbeitrag
<http://forums-de.wow-europe.com/thread.aspx?fn=wow-suggestion-de&t=139147>
- Safer Networking: Email der Review-Abteilung
reviews@spybot.info

C. Ergänzende Texte

C.1. Kommunikation an und von Blizzard

C.1.1. Forenbeitrag

Folgender Post erschien, von uns unter dem Pseudonym *Tujethirun* verfasst, am 2. März 2006 um 13:57 Uhr im deutschen *Vorschläge*-Unterforum zu World of Warcraft:

Aufgrund vielfacher Diskussionen über den ‘Warden’, der in WoW enthaltene Code zur Aufspürung von Cheats, hat sich die Safer Networking Ltd., einigen vielleicht von der recht verbreiteten Software Spybot-S&D bekannt, dieser Problematik angenommen.

Im Rahmen dieser Untersuchungen wurde ebenfalls überprüft, inwieweit sich Blizzard ganz allgemein an das Bundesdatenschutzgesetz hält.

§19 des BDSG sagt dazu:

§ 19 Auskunft an den Betroffenen

- 1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über
 1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und
 2. den Zweck der Speicherung.

Blizzard selber stimmt dem auch zu und sagt dazu folgendes:

Was können Sie tun, um Ihre persönlichen Daten einzusehen oder abzuändern?

Wenn Sie aus irgendeinem Grund genau wissen möchten, in welcher Weise wir Ihre persönlichen Daten verwenden, oder wenn Sie Informationen korrigieren oder uns die weitere Verwendung Ihrer persönlichen Daten untersagen möchten, setzen Sie sich bitte mit Blizzard unter folgender Adresse in Verbindung: Blizzard Entertainment Europe, TSA 60 001, 78143 Vélizy Villacoublay Cedex France. Sie können uns auch telefonisch unter der Rufnummer 0033 1 30 67 90 00 oder per E-Mail webmaster-de@blizzard.com benachrichtigen.

Die Safer Networking Ltd. hat nun zweimal (mit unterschiedlichen Adressen und Texten, um sicherzustellen, dass ein unglücklicher Spamfilter zuviel³³ herausfiltert) diese Anforderung per Email gestellt, jeweils mit einer Frist von 7 Tagen, ohne Antwort zu erhalten.

Bei einem Telefonat mit der angegebenen Telefonnummer war keine zuständige Person erreichbar, die von der Telefonistin auf Wunsch an diese Person geschriebene zusätzliche Email hat auch zu keiner Kontaktaufnahme geführt.

Das Kontaktformular für Rechnungsfragen akzeptierte unsere Anfrage in wiederholten Versuchen nicht.

Da Blizzard weder per Email, Telefon noch Kontaktformular reagiert, **schlagen wir nun auf diese Weise zweierlei vor:**

1. Dass andere WoW-Spieler, die diese Anfrage ebenfalls schon einmal gestellt haben, uns ihre Erfahrungen an reviews@spybot.info mitteilen.
2. Dass Blizzard diese vom Gesetz vorgeschriebene Auskunft so bald wie möglich erteilt. Zwar wird dies unsere Meldung an den Landesdatenschutzbeauftragten nicht verhindern, könnte aber zumindest das nun äußerst negative Ergebnis des Testes noch beeinflussen.

C.1.2. Formbrief von Granite, Account Administration Team

Sehr geehrter Herr Kolla,

vielen Dank für Ihre E-Mail. Unsere Hinweise zum Datenschutz können Sie

³³Es muß an dieser Stelle natürlich *nicht zuviel* heißen.

unter folgendem Link einsehen:

<http://www.blizzard.de/privacy.shtml>

Außerdem finden Sie die 'Hinweise zum Benutzerdatenschutz' in unseren Nutzungsbestimmungen unter Punkt 10:

<http://www.wow-europe.com/de/legal/termsfuse.html>

Bitte zögern Sie nicht uns zu kontaktieren sollten Sie weitere Informationen benötigen.

Mit freundlichen Grüßen

Granite
Account Administration Team
Blizzard Entertainment Europe
<http://www.wow-europe.com/de/support>

Index

Account Administration Team, [7](#), [15](#)
advapi32.dll:AdjustTokenPrivileges, [4](#)
advapi32.dll:LookupPrivilegeValueA, [4](#)

BDSG, [7](#), [14](#)
BHO, [4](#)
Blizzard, [3](#)
Browser Helper Objects, [4](#)
Bundesdatenschutzgesetz, [7](#), [14](#)

Code Injection, [3](#), [4](#)
Code-Segment, [3](#), [8](#)

Daten-Segment, [3](#)
Datenschutzvereinbarung, [7](#), [15](#)
DLL, [11](#), [13](#)

EULA, [3](#)
Export-Table, [13](#)

Forum, [7](#), [14](#)
Funktionen, [11](#), [13](#)

Granite, [7](#), [15](#)

Import-Table, [11](#)

kernel32.dll:CreateToolhelp32Snapshot, [4](#)
kernel32.dll:GetModuleFileNameA, [4](#)
kernel32.dll:GetModuleHandleA, [4](#)
kernel32.dll:Process32First, [4](#)
kernel32.dll:Process32Next, [4](#)
kernel32.dll:ReadProcessMemory, [3](#)
kernel32.dll:TerminateProcess, [4](#)
Kontaktformular, [6](#), [14](#)
Kundendienst-Kontaktformular, [6](#)

Landesdatenschutzbeauftragter, [7](#), [14](#)
Launcher, [9](#)

Nutzungsbedingungen, [10](#)

PE, [8](#)
Portable Executable, [8](#)

Protected Memory, [3](#)

RAM, [3](#)
Rechnungssupport, [6](#)
Reverse Engineering, [5](#), [9](#)

scan.dll, [11](#), [13](#)
Support-Forum, [7](#), [14](#)

Task Manager, [4](#)
Topic-ID 139147, [7](#)
TOU, [3](#)
Tujethirun, [7](#), [14](#)

UPX, [8](#)

Vélizy, [14](#)

Warden, [14](#)
Windows NT, [3](#)