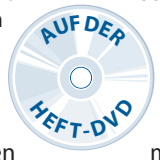
Daniel Bachfeld, Gerald Himmelein

Nagelprobe

Security-Tools für Fortgeschrittene

Das Sicherheitspaket auf der Heft-DVD bietet Tools zum manuellen Aufspüren von Malware, zum Analysieren der Stärke von Passwörtern und zum Aufdecken von Sicherheitsproblemen in Webanwendungen.

Malware schafft es immer häufiger, sich trotz installiertem Virenscanner auf Windows-PCs einzunisten und dort unerkannt ihrer schädlichen Arbeit nachzugehen. Der englischsprachige **Norton Power Eraser** von Symantec versteht sich weniger als On-Demand-Scanner, sondern vielmehr als ein Forensik-Werkzeug, das ohne die zusätzliche Installation eines weiteren Echtzeit-Scanners Klarheit verschaffen kann. Für eine Überprüfung inklusive Rootkit-Erkennung verlangt das Norton-Werkzeug jedoch gleich zu Anfang einen Neustart.

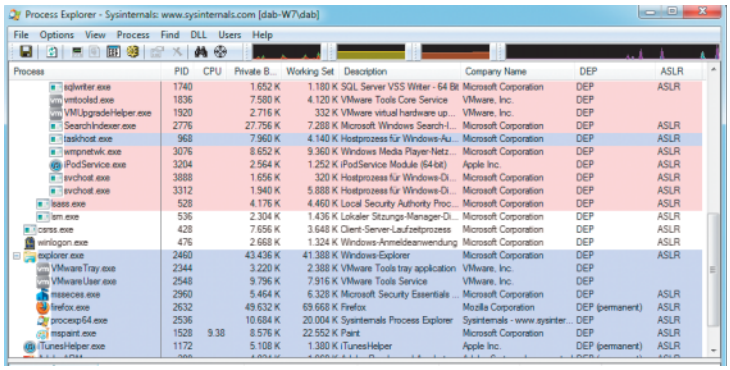


Doch Achtung: Das Tool ist nichts für schwache Nerven. Beim ersten Scan listet Power Eraser alle Prozesse auf, die ihm irgendwie verdächtig vorkommen – das bedeutet nicht zwingend eine Infektion. Alle vom Tool als „Suspicious“ markierten Prozesse sollte man unbedingt erst mit einem Remote Scan überprüfen, bevor man die „Fix“-Funktion aktiviert. Power Eraser schickt dazu verdächtige Dateien an die Symantec-Server, die sich um die weitere Analyse kümmern. Ohne Internet-Verbindung ist das Programm also nicht sinnvoll einsetzbar. „Not a known threat“ bedeutet, dass die Datei harmlos ist. Ein Klick auf den Dateinamen liefert weitere Informationen.

Wer den Verdacht hat, dass sein Rechner infiziert ist, kann sich auch selbst auf die Spurensuche begeben, statt sich auf automatische Scanner zu verlassen. Als ersten Schritt kontrolliert man, ob sich gerade laufende Prozesse irgendwie verdächtig machen, weil beispielsweise der Name der exe-Datei seltsam aussieht oder der Speicherort ungewöhnlich ist. Für diese Arbeit bietet sich der **Process Explorer** an, ein Bestandteil der legendären **Sysinternals Suite**. Der Process Explorer listet alle Windows-Dienste, Hintergrunddienste und laufende Anwendungen mit Herstellerangaben sowie einer Kurzbeschreibung auf. Ein Doppelklick auf eine Anwendung öffnet die Eigenschaften, in der im Reiter TCP/IP aktive Netzwerkverbindungen ersichtlich sind. Zur Sysinternals Suite gehört auch **Autoruns**, mit dem sich alle Möglichkeiten anzeigen lassen, wie ein Programm, Skript oder eine Bibliothek unter Windows automatisch gestartet werden kann.

Startete Malware früher über Run-Keys in der Registry, klinkt sich etwa Scareware heutzutage gut versteckt etwa als „Layered Service Provider“-Komponente (LSP) in eine Netzwerkverbindung ein und überwacht, ob ein Anwender bestimmte Seiten aufruft. Autoruns kann solche unerwünschten Einträge im Reiter „Winsock Layered Service Providers“ anzeigen. Der Anwender muss die Ergebnisse sowohl von Autoruns als auch vom Process Explorer und deren Relevanz hinsichtlich einer Infektion selbst richtig interpretieren können. Alternativ zu Autoruns

liegt das Tool **RunAlyzer** der Entwickler von Spybot Search&Destroy auf der Heft-DVD bereit. Einige Autostart-Mechanismen zeigt das Tool zwar nicht an, dafür listet es aber übersichtlich die für den Internet Explorer geladenen Plug-ins und Einträge unter „geplante Ereignisse“ (scheduled Tasks) auf. Will man einem Programm noch genauer auf die Finger schauen, liefert Sysinternals’ **Process Monitor** eine Übersicht aller Datei- und Registry-Zugriffe. Allerdings überflutet einen das Tool mit Informationen, sodass man ohne vernünftige Filter lange mit der Analyse zubringt.



Mit dem Process Explorer kommt man nicht nur Malware auf die Spur, sondern auch Systembremsen, die unnötig Speicher und CPU-Ressourcen in Beschlag nehmen.

Am besten präventiv benutzt man das Windows-Programm **TrackWinstall**. Es protokolliert Änderungen am System, wie sie Installationsprogramme oder auch Schädlinge vornehmen. Dazu erfasst TrackWinstall zunächst den Ausgangszustand der Windows-Registry und des Dateisystems. Anschließend startet TrackWinstall die Installation des gewünschten Programms, überprüft danach Registry und Dateisystem auf Änderungen und zeigt diese an. Leider zeigt das Tool sämtliche Änderungen an, die vom letzten gemerkten Zustand bis zur erneuten Prüfung aufgetreten sind, und darunter können auch Änderungen sein, die nicht auf die Installation zurückzuführen sind.

Mit Rootkits versuchen Malware-Autoren, die Aktivitäten ihrer Bots und Trojaner zu verstecken. Zu der Malware gehörende Prozesse tauchen dann etwa im Task Manager oder auch im Process Explorer nicht mehr auf. Rootkits kommt man jedoch mit dem **Rootkit Revealer** aus der Sysinternals Suite, **GMER** und **Sophos Anti-Rootkit** auf die Schliche. Hat man den Verdacht, dass ein dubioses Programm unerwünschte Netzwerkverbindungen aufbaut, kann man sich den Datenverkehr mit dem Netzwerkanalysator **Wireshark** näher anschauen. Damit lässt sich beispielsweise herausfinden, ob ein Bot Spam-Mails verschickt oder mit einem Command&Control-Server Kontakt aufnimmt.

Oft verraten sich Bots durch den Verbindungsaufbau zu einem Channel auf einem IRC-Server oder zu einen Webserver. Zwar verschlüsseln viele Bots ihre Kommunikation, aber allein der Kontakt zu solch einem Server kann bereits Hinweis genug sein. Um die beim Sniffen aufkommende Datenmenge zu reduzieren und zu verhindern, dass unschuldige Update-Prozesse ins Visier geraten, sollte man vor dem Start von Wireshark alle Online-Anwendungen und Update-Dienste beenden. Wireshark benötigt **WinPCap**, das bereits in der Installationsdatei enthalten ist und mitinstalliert wird.

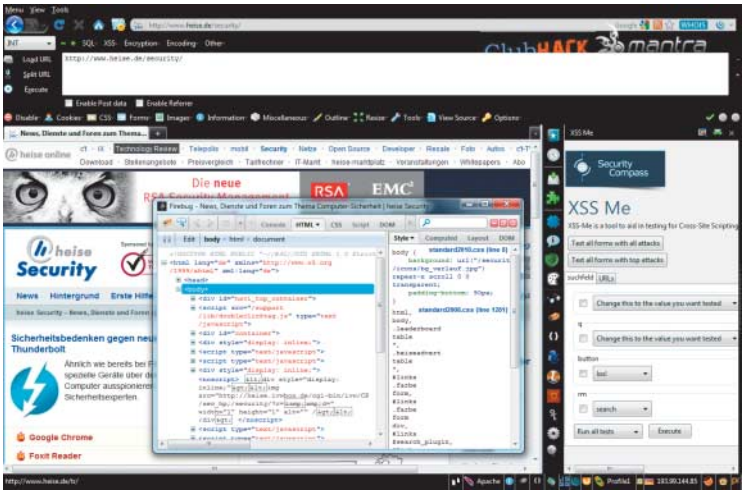
Wem Wireshark mit seinen vielen Optionen zu unübersichtlich ist, der sollte **SmartSniff** ausprobieren. SmartSniff konzentriert sich im Wesentlichen auf einen Start- und Stop-Knopf zum Sniffen sämtlicher vorbeikommender TCP-, UDP- und ICMP-Pakete. Anders als Wireshark zeigt SmartSniff aber nicht jedes Paket einzeln an, sondern stellt die Informationen verschiedener GET-Requests und Server-Antworten beispielsweise im Kontext einer HTTP-Verbindung dar. Wem selbst das zu unübersichtlich ist, der kann sich mit **SocketSniff** auf das Sniffen der Netzwerkverbindung einzelner Prozesse konzentrieren. Beim Start präsentiert das Tool eine Liste von Prozessen, aus der man einen zur Überwachung auswählen kann. In einem Fenster zeigt SocketSniff dann Quell- und Zieladresse mitgelesener Pakete sowie Ports und Paketgröße an. Ein Klick auf ein Paket präsentiert in einem weiteren Fenster den Inhalt wahlweise in ASCII- oder Hex-Darstellung.

Mitunter stößt man bei der Analyse eines Systems auf Dateien, die keine Endung haben und sich auch mit den üblichen Bordmitteln nicht öffnen lassen. **Filealyzer** bietet nach der Installation im Kontext-Menü des Windows Explorer zusätzlich Punkte, etwa um eine Datei als Hexdump anzuzeigen oder enthaltene Strings, Zertifikate sowie MD5- und SHA-1-Prüfsummen anzuzeigen. Bei ausführbaren Dateien versucht das Tool zudem, die verwendete Programmiersprache zu erraten. Unter NTFS kann es Alternate Data Streams aufspüren, also zusätzliche, dem Anwender in der Regel verborgene Speicherbereiche.

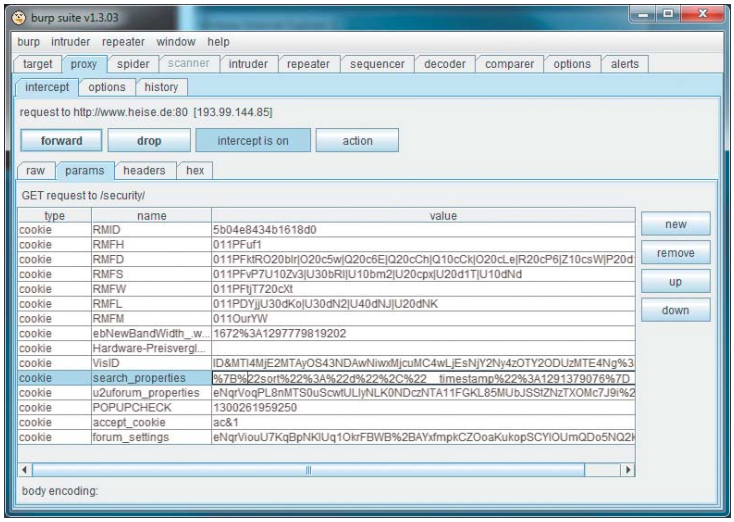
Virenautoren komprimieren Malware oft oder verschlüsseln sie sogar, um sie der Analyse durch Virenscanner zu entziehen. **PEiD** gibt Hinweise, welchen Packer oder Crypter ein Autor für seine ausführbare Datei benutzt hat. Ein seltener Packer wie Amarillo kann etwa ein Hinweis für Malware sein, muss es aber nicht. Zudem zeigt PEiD an, mit welchem Compiler das untersuchte Programm erstellt beziehungsweise in welcher Sprache es geschrieben wurde. Mit dem Tool lassen sich Programme auch schnell disassemblieren und deren Funktion nachvollziehen, wobei man per Doppelklick JMPs und CALLs folgen kann. Sinnvoll ist dies jedoch nur bei kleinen Programmen, bei größeren sollte man lieber dedizierte Debugger einsetzen.

Vorsorge

Die genannten Tools kommen normalerweise erst zum Einsatz, wenn das Kind schon in den Brunnen gefallen ist und sich ein Sicherheitsproblem akut auswirkt. Es gibt aber auch Tools, um die Sicherheit vorab zu überprüfen und gegebenenfalls Schwachstellen zu beseitigen. **Cain&Abel** ist beispielsweise solch ein Tool, mit dem sich die Stärke von Passwörtern prüfen lässt – indem man versucht, sie zu knacken. Der Passwort-Cracker kann etwa anhand von NTLM-, MD5, SHA1- und diversen andere Hashes ein Passwort errechnen. Dazu geht er Wörterbücher durch oder probiert per Brute-Force-Attacke Kombinationen durch. An die zu knackenden Daten gelangt das Tool durch das Auslesen lokaler Daten oder durch das Abhören der Netzwerkkommunikation mit seinem eingebauten Sniffer. Weil in geswitchten Netzwerken das Belauschen der Verbindungen anderer Systeme nicht ohne Weiteres möglich ist, unterstützt das Tool ARP-Cache-Poisoning



Das Mantra Security Toolkit hat einen mächtigen Funktionsumfang. In der Bedienoberfläche verliert man jedoch so manches Mal den Überblick.



Mit dem Burp-Proxy lassen sich bereits mit dem Browser abgesendete Formulare abfangen und nachträglich ändern.

zum Umleiten von Verbindungen über den eigenen Rechner.

Cain&Abel kann für Man-in-the-Middle-Attacken etwa auf SSL-gesicherte Verbindungen gefälschte Zertifikate erzeugen und einem Client präsentieren. Zudem filtert das Tool übertragene Passwörter gleich aus und speichert belauschte VoIP-Gespräche als Sound-Datei ab. Cain&Abel unterstützt auch das Mitschneiden von WPA-Handshakes im WLAN, um anschließend schwache WPA-PSKs zu knacken.

Einen Überblick über alle Systeme im LAN daheim und deren offene Ports liefern der Port-Scanner **Nmap** und seine grafische Oberfläche **Zenmap**. Zenmap ist insbesondere in größeren Netzen nützlich, um eine Übersicht über Rechner und Netze zu erhalten. Nmap selbst beschränkt sich schon längst nicht mehr auf das Finden offener Ports, sondern bietet dank seiner Nmap Scripting Engine (NSE) die Möglichkeit, Systeme auf bestimmte Schwachstellen zu untersuchen. Eines der letzten Updates enthielt sogar ein Skript, um aus der Ferne eine Stuxnet-Infektion eines Systems aufzudecken. Daneben gibt es fast 200 weitere Skripte, mit denen man verschiedene Dienste und Server wie HTTP, IMAP, SMB und SMTP auf diverse Lücken untersuchen kann.

Wer Webanwendungen jedoch intensiver auf ihre Widerstandsfähigkeit gegen manipulierte Eingaben, Cross-Site-Scripting, SQL-Injection und vielerlei andere Angriffe testen möchte, sollte das **Mantra Security Toolkit** (MST) ausprobieren. Damit können Webentwickler Fehler provozieren und so Sicherheitslücken in ihren Webanwendungen aufspüren. Daneben ist das Toolkit aber auch geeignet, um bösartige Webseiten zu untersuchen, die etwa per Exploit versuchen, einen PC zu infizieren. Das Toolkit ist im Wesentlichen ein modifizierter, mit mehr als 40 Add-ons gespickter Firefox-Browser, der sich parallel zu einem bereits installierten Firefox betreiben lässt. Im Hauptfenster zeigt MST die gerade aufgerufene Seite, die Bedienoberfläche der Add-ons öffnet sich entweder in einer Sidebar oder einem separaten Fenster.

Zu den Add-ons gehören bekannte wie Live HTTP Header, FireBug, JSView und Dom Inspector, mit denen sich abgerufene HTML-Dokumente analysieren und eigene Request erstellen lassen. Die Add-ons „SQL Inject Me“ und „XSS Me“ versuchen automatisch, in Eingabefeldern einer Webseite SQL-Injection- und Cross-Site-Scripting-Lücken zu entdecken. Daneben finden sich Add-ons zum Manipulieren von Cookies und HTTP-Requests. Wie man gefundene Fehler in seiner Webanwendungen repariert, zeigt unter anderem das auf der Heft-DVD beiliegende E-Book „PHP-Sicherheit“.

Beim Untersuchen von Webseiten leistet auch die einzige für den Internet Explorer verfügbare Erweiterung **DebugBar** gute Dienste. Sie liefert Informationen über die URLs von nachgeladenen Elementen, derzeit aktive Skripte, den bereits interpretierten HTML-Code und vieles mehr.

Mit sogenannten HTTP-Debugging-Proxies kann man ebenfalls den Verkehr zwischen Browser und Server analysieren und manipulieren, allerdings unabhängig vom verwendeten Web-Client. Die **Burp Suite Free Edition** schaltet sich als Proxy in die Client-Server-Verbindung und zeigt jeden GET- oder POST-Request übersichtlich mit seinen Parametern an. Dabei ist es dem Tester möglich, jeden Request eines Clients abzufangen und erst nach einer Freigabe an den Server weiterzusenden. Auf diese Weise lassen sich Werte von gesendeten Parametern nachträglich ändern. Die Burp Suite hilft auch beim Debugging von SSL-Verbindungen und präsentiert dem Client ein automatisch selbst erstelltes Zertifikat. Dabei ist der Proxy in der Lage, on the fly ein SSL-Zertifikat für den gerade angefragten Hostnamen zu erstellen. Das provoziert zwar im Client einen Fehler, importiert man jedoch das Wurzelzertifikat der Burp Suite etwa in den von der Anwendung verwendeten Schlüsselring, so meckert der Client künftig nicht mehr. Auf diesem Weg lassen sich nicht nur eigene Anwendungen debuggen. Auch die verschlüsselt gesendeten Inhalte von Anwendungen anderer Hersteller lassen sich kontrollieren – falls man deren Angaben, etwa dass niemals vertrauliche Daten verschickt werden, nicht ganz traut. Die Burp Suite kann als lokaler oder externer Proxy arbeiten und benötigt Java.

Ohne Java, dafür aber nur unter Windows arbeitet der Proxy **Fiddler**. Er weist einen ähnlichen Funktionsumfang wie die Burp Suite auf, kann aber beispielsweise Anfragen an einen Server umbiegen und stattdessen lokal gespeicherte HTML-Seiten ausliefern. Mit FiddlerScript lassen sich Requests und Antworten sogar automatisch umschreiben, etwa um bestimmte Tags auszufiltern. **FiddlerCap** ist ein Werkzeug, das nur zum Mitschneiden von HTTP-Verkehr dient. Die Daten lassen sich später mit Fiddler laden und analysieren. Das ist praktisch, wenn man bei einem Bekanntem aus der Ferne einem Problem auf den Grund gehen will, dem jedoch die Bedienung von Fiddler schon zu komplex ist. (dab)

Security-Leseecke

Viele populäre Webanwendungen sind in PHP programmiert, viele davon leider auch unsicher. Das im dpunkt-Verlag erschienene E-Book **PHP-Sicherheit** von Christopher Kunz und Stefan Esser zeigt Programmierern, welche Sicherheitsprobleme es gibt und wie man diesen begegnet. Auf 335 Seiten erfährt der Leser Details über SQL-Injection, Cross-Site-Scripting und Cross-Site-Request-Forgery und wie man diese Angriffe programmiertechnisch ins Leere laufen lässt. Zwei Kapitel widmen sich den Interna der Sicherheitseinstellungen von PHP und der PHP-Sicherheitserweiterung Suhosin zum Härten von Server-Systemen.

Daneben finden sich auf der DVD Auszüge aus drei Büchern des dpunkt-Verlages mit jeweils mehreren Kapiteln. Dazu gehört **Aus dem Tagebuch eines Bughunters. Wie man Softwareschwachstellen aufspürt und behebt** von Tobias Klein, das an sieben Beispielen demonstriert, wie der Autor Software unter verschiedenen Betriebssystemen untersucht. **Computer-Forensik** von Alexander Geschonnek gibt einen Überblick darüber, wie man bei der computerforensischen Arbeit vorgeht und etwa Beweisspuren gerichtsverwertbar sichert. Der noch nicht im Buchhandel erschienene Leitfaden **Penetration Testing mit Metasploit: Eine praktische Einführung** von Frank Neugebauer zeigt, wie man das Exploit-Framework Metasploit installiert und konfiguriert und in einer Testumgebung einsetzt.

c't