

Anti Forensik Techniken – wenn Bedarfsträger in die Röhre schauen

News Summary

Anti Forensik Techniken wurden in den letzten Jahren abseits der öffentlichen Wahrnehmung entwickelt und erblickten etwa Ende 2005 des Licht der informationsverarbeitenden Welt. Dabei wurden sie in eine fruchtbare Umgebung hinein geboren: Zum einen fehlte es im Bereich der Entwicklung von Forensik-Werkzeugen zu dieser Zeit an wirklich innovativen Neuerungen und zum anderen war eine deutliche Abhängigkeit der forensischen Ermittlung von den jeweils eingesetzten Softwaretools zu konstatieren. Nunmehr haben Anti Forensik Techniken einen Entwicklungsstand erreicht, der herkömmliche forensische Werkzeuge von Ermittlungsbehörden und privatwirtschaftlichen Unternehmen in Bedrängnis zu bringen vermag. Nur wenige dieser Techniken werden dabei uneingeschränkt der breiten Öffentlichkeit zugänglich gemacht. Vielmehr besitzt die sog. Underground Economy nur ein geringfügiges Interesse an der öffentlichen Verbreitung entsprechender Tools, welche regelmäßig in Anlehnung an den originären Angriffsvektor quasi als Nebenprodukt des Bemühens um die Kompromittierung von Hard- oder Software entstehen. Außerhalb des szenetypischen Non Disclosures vollzog sich dagegen die Entwicklung des sog. Metasploit Anti-Forensic Investigation Arsenal (MAFIA), welches auf der Grundlage einer Schwachstellenanalyse verschiedene Anwendungs- und Implementierungsfehler forensischer Werkzeuge wie Encase, AccessData Forensic Toolkit, X-Ways Forensics, iLook, Sleuthkit oder Autopsy lokalisiert und sodann für eigene Zwecke nutzt.

Grundsätzlich fokussieren Anti Forensik Techniken nicht originär auf die Erlangung des Zugangs zum Informationssystem des jeweiligen Opfers an sich (bspw. durch die Ausnutzung der gefundenen Schwachstellen durch Exploits o.Ä.), sondern vielmehr auf die Beeinflussung des Ergebnisses einer forensischen Untersuchung i.R. der Erkenntnisgewinnung durch den jeweiligen Bedarfsträger. Exploits, wie sie bspw. im MAFIA zu finden sind, sind dabei nur eine Möglichkeit, Spuren eines sanktionalen Verhaltens auf informationsverarbeitenden Systemen zu verwischen. Dr. Marcus Rogers, Wissenschaftler an der Purdue University, klassifizierte die Angriffe auf AF-Tools wie folgt: [1] Löschen/Verbergen von Daten (durch Rootkits, Kryptografie und Steganografie), [2] Vernichten von nebenläufigen Informationen, den sog. Artefakten (durch sog. Disc Cleaner etc.), [3] das Verwischen von Spuren (durch Spoofing oder Desinformation) sowie [4] Angriffe gegen softwareimplementierte und standardisierte Prozesse von Computerforensik-Tools (Änderung der Dateisignatur, Fälschung von Hashwerten etc.).

Obgleich die Hersteller der einschlägigen Produkte ständig bemüht sind, Schwachstellen in den eigenen forensischen Werkzeugen zu beseitigen, lassen die Tools des MAFIA erahnen, dass diesbezüglich noch viel Raum für kreative Entwicklungen existiert. Zum Schutz ihrer Produkte gehen die Hersteller verschiedene Wege: Während die einen die Entwicklung von Anti Forensik Tools mehr oder weniger zu behindern versuchen, lud Guidance Software (der Hersteller von Encase) dagegen die Metasploit-Entwickler als Gastredner auf ihre Konferenzen ein. Augenscheinliches Motto dieses „Umwerbens“ der Metasploit-Macher: Wenn wir schon nicht antizipiert auf die Entwicklung des MAFIA Einfluss nehmen können, so kommen wir auf diese Weise zumindest zeitnah an die entsprechenden Informationen über die Schwachstellen unserer eigenen Produkte heran.

Anti Forensik Tools werden heute regelmäÙig als für den "Normalnutzer" nur schwierig zu bedienende Kommandozeilen-Tools angesehen, die i.E. keine ernsthafte Bedrohung für etablierte forensische Werkzeuge darstellen. Das Gegenteil ist allerdings der Fall: Mittels des Timestomp Exploits des MAFIA kann bspw. die Fähigkeit forensischer Werkzeuge zur Ermittlung der Timestamps von Dateioperationen kompromittiert werden. Die Folge: Eine Zurechnung einer deliktischen Handlung ist mit der notwendigen Verurteilungswahrscheinlichkeit letztlich nicht mehr möglich. Auch verlassen sich die Cyberforensiker immer noch gern auf die (vermeintliche) Unwissenheit der Nutzer. So äußerte sich Simon Janes, der Gründer der Forensic Alliance, zur Frage inwieweit Artifact Wiping Tools die Arbeit der Computerforensiker erschweren würden, wie folgt:

>There are lots of tools out there for wiping hard drives. The first thing is don't be intimidated by the fact they've been used. They are often used by people who don't understand how they work so you can normally find something.</div>

Wohin der "Cyberforensik-Zug" fahren wird, ist noch nicht klar. Schaut man allerdings auf die Website des Metasploit-Projektes, bekommt man eine leise Ahnung von den zukünftigen Möglichkeiten der Anti Forensik: Modifikation des NTFS-Journalings, sichere Lösungsverfahren, Manipulation der Browser Logs sowie Modifikation der Metadaten von Files. Ruhige Zeiten scheinen den Herstellern von Forensik-Tools also nicht verfallen zu sein. Im Ergebnis kann derjenige, der wirklich etwas zu verbergen hat, auf ein schier grenzenloses Repertoire von Technologien zur Informationsvermeidung und -unterdrückung zurückgreifen, ohne das je ein Bedarfsträger den wahren Inhalt eines Datenblocks zu Gesicht bekommt. Die einfältige Vorstellung, mittels Onlinezugriffs auf Datenträger die vorbenannten Probleme der "Offline-Ermittlung" kompensieren zu können, wird gerade in Hinsicht auf die anvisierte Zielgruppe und die zur Verfügung stehenden Technologien zur Lachnummer. Virtualisierungstechniken erlauben jedem PC-Anwender ohne besondere Kenntnisse und Fähigkeiten eine Vielzahl von virtuellen Maschinen auf einem physischen Host zu beheimaten. Zukünftig wird also für die notwendigen "Online-Ange" eine virtuelle Maschine abgestellt, eine andere wird zur Verwaltung des lokalen Filearchivs benutzt, eine dritte wiederum dient zur Erledigung der terroristischen Anschlagplanung. Auf den virtuellen Maschinen wird darüber hinaus ein Biotop verschiedener Betriebssysteme entstehen "Monokulturen und die damit einhergehenden Gefahren werden immer weiter zurückgedrängt. Konzeptionsverfahren werden die Herrschaft über Filesysteme und Datencontainer übernehmen.

Die Innen- und Sicherheitspolitik ist gekennzeichnet durch Aktionismus und Symbolik. Entsprechende Normkonvolute erreichen den ihnen angetragenen Gesetzeszweck zumeist nur fragmentarisch. Andererseits scheint die Zweckerreichung eines Sicherheitsgesetzes zwischenzeitlich so und so zum nebenläufigen Aspekt zu verkommen. Vielmehr besteht augenscheinlich ein eigentümlicher Konsens zwischen den "Sicherheitsexperten" der Regierungsparteien dahingehend, dass man zu Gunsten der Sicherheit die Freiheit ohne Wenn und Aber zur Schlachtbank führen muss. Während allerdings Schily noch zurückhaltend und dennoch wahrnehmbar Opfergaben auf dem Altar der Sicherheit erbrachte, sind Schäuble, Beckstein, Bosbach, Wiefelspütz, Zierke und Co. einem wahren Blutausch erlegen, in dem sie nunmehr wahrlich alle Grundfreiheiten zu schlachten bereit sind, um dem Volk die Sicherheit zu geben, die es verdient.

weiterführende Links

[Leitseite smartnuts.com](#)

[Urteilsdatenbank smartnuts.com](#)

www.smartnuts.com