Cybergefahr

Wie wir uns gegen Cyber-Crime und Online-Terror wehren können

Bearbeitet von
Eddy Willems

1. Auflage 2015. Buch. XVIII, 188 S. Softcover
ISBN 978 3 658 04760 3
Format (B x L): 16,8 x 24 cm

Weitere Fachgebiete > EDV, Informatik > Hardwaretechnische Grundlagen > Computerkriminalität, Schadsoftware

Zu Inhaltsverzeichnis

schnell und portofrei erhältlich bei

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Profile der Malware-Verfasser

2

2.1 Die Graffiti-Sprayer und Script-Kids

Die ersten Viren und Würmer wurden von Teenagern und Studenten geschrieben, die es einfach nur interessierte, wie schnell sie ihren Virus in die große weite Welt hinausschicken konnten. Böse Absichten versteckten sich dahinter fast nie. Sie legten den Grundstein bis ca. 2006, schrieben aber eigentlich den geringsten Teil der Malware. Allerdings bildeten sie die größte Gruppe der Malware-Schreiber. Aber auch in den Anfangsjahren waren sie nicht die Einzigen, bereits damals waren Cyberkriminelle aktiv.

Weil sie technisches Talent bewiesen und damit angeben wollten, nenne ich sie auch heute noch „Script-Kids“. Damals wurde Malware oftmals über Copy und Paste der im Internet gefundenen Scripte weitergeleitet. Dies dürfte auch der Grund für deren schlechte technische Qualität gewesen sein und Antivirenprogramme hatten meist kaum Probleme mit der Beseitigung. Diese Malware findet man heute gelegentlich noch – sie spiegelt aber lange nicht mehr den aktuellen Stand der Möglichkeiten wider.

2.2 Die Cyberkriminellen

Während dieses Buch geschrieben wurde, war diese Gruppe für 99 % der Malware verantwortlich. Und sie tut es nur aus einem einzigen Grund: Geld. Wir werden uns in Kap. 3 über die Wirtschaft der Unterwelt noch intensiv mit diesem Thema befassen. Die technische Expertise der Cyberkriminellen wird zunehmend besser.

© Springer Fachmedien Wiesbaden 2015

E. Willems, *Cybergefahr,* DOI 10.1007/978-3-658-04761-0_2

2.3 Die unwissend Böswilligen

Diese relativ kleine Gruppe will nur ihre Programme und Daten schützen, setzt hierzu aber Software ein, die wiederum von Dritten mit weniger guten Absichten genutzt werden kann. Das Sony-Rootkit aus dem vorherigen Kapitel illustriert das recht anschaulich. Aber auch so manche Aktionen unterschiedlicher Ministerien bei der Bekämpfung von Cyberkriminalität, auf die ich in Kap. 11 eingehe, fallen in diese Kategorie.

2.4 Die Behörden und Ministerien

Viele Staaten haben spezielle Institutionen gegründet, um Cyberangriffe auf ihre zivile oder militärische IT-Infrastruktur durch andere Nationen oder Cyber-Terroristen abwehren zu können. Inzwischen dürfte aber wohl niemand mehr daran zweifeln, dass die meisten Länder Malware auch einsetzen, um andere Nationen zu bespitzeln oder gezielte Attacken auf „feindliche" Ziele zu verüben. In Kap. 4 werden wir diese Aktivitäten aufdecken.

2.5 Und was ist mit den Hacktivisten?

Hier liegt der Fall etwas komplizierter. Eigentlich sind die Hacktivisten, wie das Wort suggeriert, Hacker und keine Malware-Schreiber. Als Hacker reicht es nicht, nur Schadcode zu schreiben – ganz andere Fähigkeiten werden verlangt. Oftmals ist der Hacker zwar auch ein Malware-Schreiber, aber grundsätzlich sind es unterschiedliche Personen, die als Team zusammenarbeiten. Hacker sind auf das Eindringen und/oder Lahmlegen von Webseiten und/oder Netzwerken spezialisiert, während sich Malware-Entwickler auf die Verbreitung ihres Codes konzentrieren. Sie können dabei durchaus auch „Aktivisten" sein, die Malware zu einem „höheren Ziel" einsetzen wollen oder um der Welt eine Botschaft zu verkünden.

Der Verfasser des Urvirus

Der erste Virus datiert auf das Jahr 1986, aber auch der erste Verfasser? Nun ja, genau genommen natürlich schon, aber dieser „Erfindung" sind ja verschiedene jahrelange Versuchsreihen – die Virusprähistorie sozusagen – vorausgegangen. Sie werden in dem großartigen Nachschlagewerk von François Pagets mit dem Titel Vers &Virus (Wurm und Viren) beschrieben. Einige Höhepunkte möchte ich Ihnen natürlich nicht vorenthalten.

Der ungarisch-amerikanische Wissenschaftler John von Neumann schrieb viele revolutionäre Beiträge, er dürfte aber auch durch seine Rolle im Manhattan-Projekt, das zur ersten Atombombe führte, bekannt sein. Seine Analyse der Struktur selbstreplizierender Organismen hat indirekt zur Entdeckung der DNA-Struktur geführt. Allerdings

hat sie auch zur Erfindung eines Virus oder Wurms in Form eines digitalen Organismus beigetragen, der in der Lage ist, sich selbst zu reproduzieren.

Im Jahr 1971 entdeckten wir ein erstes Programm, das sich wie ein Wurm verhielt. Es hieß damals Creeper, konnte sich von Computer zu Computer bewegen und diente quasi als Übungswerkzeug für die Luftverkehrsleitung: Immer dann, wenn sich das Programm in einen Computer einnistete, erschien auf dem Bildschirm des jeweiligen Computer: „I'm creeper! Catch me if you can!" Nachfolgende Versionen von Creeper konnten sich sogar fortpflanzen. Später wurde dann Reaper entwickelt, um alle Creeper zu entfernen. Es ist ein wenig wie ein Katz-und-Maus-Spiel, das Wurm und Antivirus jahrelang durchhalten.

Last but not least möchte ich den Science-Fiction-Autor David Gerrold, der unter anderem an der Star Trek-Reihe mitgeschrieben hat, nicht unerwähnt lassen. In seinem Roman When HARLIE was one wird HARLIE (Human Analogue Robot Life Input Equivalents) als ein Computer mit stark entwickelter künstlicher Intelligenz beschrieben, der mit anderen Computern in Kontakt treten kann, um sie neu zu programmieren oder ihre Daten zu ändern. Um den Kontakt herzustellen, nutzt er ein Programm, das nach Zufallsprinzip Nummern anwählt, in der Hoffnung, dass die Nummer einem anderen Computer gehört. Sobald ein Computer gefunden ist, wird das Programm auch auf diesen Computer geladen. Der Name des Anwählprogramms? Ganz einfach: Virus.

2.6 Gigabyte: Made in Belgium

Auch die „öffentlichste Botschaft" eines Viren-Schreibers kann manchmal sehr persönlich sein. Betrachten wir einmal die Geschichte der allerersten – zumindest soweit wir wissen – weiblichen Malware-Entwicklerin der Welt mit dem „Künstlernamen" Gigabyte. Diese – man höre und staune – Belgierin beschäftigte sich bereits seit längerer Zeit experimentell mit Viren, als sich der renommierte Virenjäger Graham Cluley ausgesprochen herablassend und überheblich über Viren-Schreiber äußerte. Daraufhin begann Gigabyte aus Rache Viren zu schreiben, die spezielle Nachrichten für Cluley enthielten.

Gigabyte war der Prototyp eines Graffiti-Sprayers (auf dem Höhepunkt ihrer „Karriere" war sie ungefähr achtzehn Jahre alt), ohne jede kriminelle Intention. Sie verbreitete Viren nie selbst, sondern setzte sie auf ihre Webseite, sodass Dritte sie zur Verbreitung nutzen konnten. Paradoxerweise gab es auf der Seite einen Warnhinweis (s. Abb. 2.1), der besagte, dass es nicht erlaubt sei, die Viren in krimineller Absicht herunterzuladen.

Journalisten der damaligen Online Station TechTV wiesen sie auf die Widersprüchlichkeit dieser Situation hin: Wer eine Waffe anderen zur Verfügung stellt, muss davon ausgehen, dass es jemanden gibt, der sie nutzt. Sie zuckte daraufhin nur mit den Schultern und gab die Schuld an die User weiter: „wenn die so blöd sind … " Die Schuld anderen zuzuschieben, war typisch für sie. Microsoft war ja auch selbst schuld, dass es so einfach war, Viren für die Windows-Plattform zu schreiben. Als Microsoft zum Gegenangriff mit

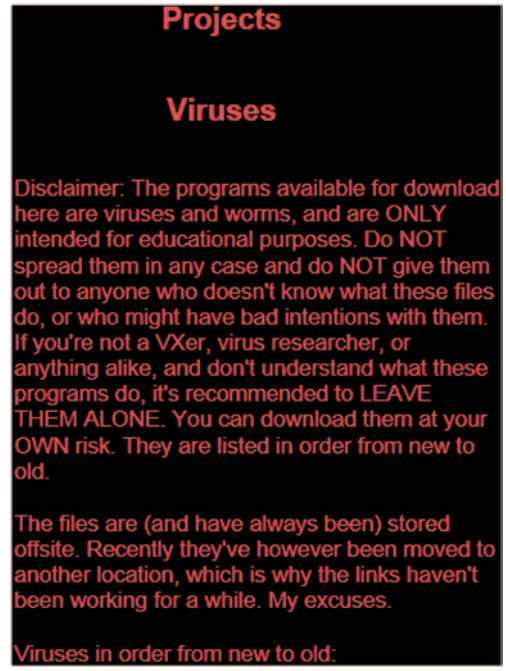


Abb. 2.1 Gigabyte Disclaimer: „Diese Viren sind NICHT zur Verbreitung vorgesehen“

dem Namen *Trustworthy Computing* ausholte, sah sie hierin lediglich einen hinterhältigen Plan, noch mehr Menschen an Microsoft zu binden. *„Conclusion: Bill Gates is Satan“* schlussfolgerte sie triumphierend (s. Abb. 2.2).

Und doch war sie, so stellte ich später fest, eine geradezu schüchterne, liebenswerte junge Frau (siehe auch Absatz „Zufällig demaskiert“ in Kap. 2.7), für die das Schreiben von Viren vor allem ihre eigene Ausdruckform war, sich zu behaupten, keinesfalls aber mit der Absicht, anderen zu schaden oder sie zu verletzen. Sie wurde verhaftet und verhört und schwor daraufhin, nie wieder Viren zu schreiben oder sich mit Malware zu befassen. Soweit ich weiß, hat sie sich an ihr Versprechen gehalten.

2.7 Virenschreiber und Virenjäger

Vor zwanzig Jahren hätte ich das nicht zu schreiben gewagt. Lange Zeit war es absolut verpönt in der Antivirenwelt, den Kontakt zu Verfassern von Viren und Malware zu suchen. „Kontakt mit dem Feind zu suchen, das gehört sich nicht“ war der damals geltende Leitsatz. Und doch kann genau das tiefe Einblicke in die Psyche und Denkweise der Malwareschreiber ermöglichen, von denen man bei der Bekämpfung von Malware profitiert. Dr. Sarah Gordon ist in verschiedenen Artikeln für Antivirus- und andere Fachzeitschriften auf diese Thematik eingegangen. Sie profitierte aus ihren Kontakten und kam zu folgenden Erkenntnissen:


them. But I can not believe that Microsoft and Intel don't realize just how evil their plan is. I don't think they're stupid enough to do the world a favour. It seems like they're not only trying to get even more customers, but to get such severe influence on daily life, that it could be called "taking over the world".
Conclusion: Bill Gates is Satan.

September 17, 2003: I finally updated the Links page, as it was full of broken links. Lots of people mailed me, asking for links on virus writing, programming etc., so I hope there's something useful for them on the page. The projects page was also updated.

September 11, 2003: I have a slight idea what I wanna work on next (when it comes to viruses), but don't expect me to hurry up :)

September 10, 2003: Had my hair dyed dark blue, almost black, for a change.

Sign My Guestbook View My Guestbook

Abb. 2.2 Aus Gigabytes Tagebuch: „Bill Gates is Satan“

1. Den typischen Virenschreiber gibt es nicht! Es sind nicht alle einsame Nerds, die ihre Intelligenz unter Beweis stellen wollen. Allerdings war die Mehrheit der Virenschreiber seinerzeit männlich, zwischen 13 und 26 Jahre alt und entwickelte aus ganz individuellen Gründen Viren.
2. Die wichtigsten Triebfedern der Virenschreiber: der Drang nach Anerkennung, die technische Herausforderung, das Verlangen, einer bestimmten Gruppe anzugehören, Rache, Neugier und das befriedigende Gefühl, wenn man nachweisen konnte, dass ein System nicht wasserdicht war.
3. Strengere Gesetze greifen kaum, um Virenschreiber von ihrem Tun abzubringen, es sei denn, sie bekommen wirklich zu spüren, dass diese Gesetze auch konsequent durchgesetzt werden. Wird jemand verhaftet, aber erst nach Monaten oder sogar Jahren verurteilt, lässt dies die Virenschreibergemeinschaft ziemlich kalt. Will man sie auf andere Gedanken und Hobbys bringen, führt kein Weg daran vorbei, ihnen klarzumachen, dass Viren nicht cool sind!
4. Werden Virenschreiber aktiv, ist ihnen meist gar nicht bewusst, dass sie etwas Böses tun. Sie verdrängen diese Tatsache und suchen nach Entschuldigungen in Phrasen wie „nur zu Forschungszwecken“ und „Haftung für Malware ist ausgeschlossen“.
5. Die Erkenntnis, erheblichen Schaden durch die eigenen Taten zu verursachen, reift erst mit zunehmendem Alter. Sarah Gordon musste leider feststellen, dass die Betreffenden immer älter sind, wenn ihnen die Folgen ihrer Machenschaften klar werden – früher bereits mit 21, jetzt erst mit 25. Wohl gemerkt: Ich rede hier von Hobby-Virenschreibern, nicht von den wahren Cyberkriminellen. Auf sie gehe ich im nächsten Kapitel ein.

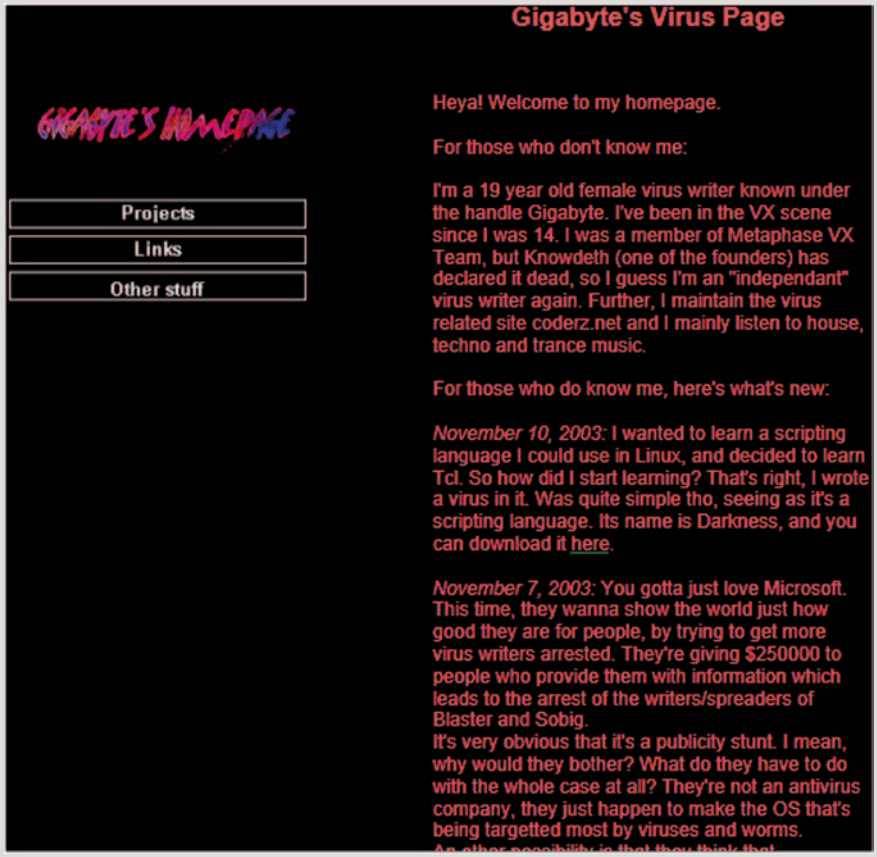
Es kursieren jede Menge Missverständnisse über das komplexe Verhältnis zwischen Virusschreibern und Virusjägern. In Kap. 7.12 werden wir sie näher beleuchten.

Aus dem Tagebuch

Zufällig demaskiert

Mai 2002

Die Homepage von Gigabyte



Ehrlich gesagt fasziniert mich der Werdegang der belgischen Virenschreiberin Gigabyte. Sie wurde ins Fernsehen eingeladen, um von ihrer Motivation, Viren zu schreiben, zu erzählen (von dem oben bereits erwähnten Fernsehsender TechTV, einem Sender aus San Francisco, der sich auf Technik und Internet spezialisiert hatte und in 73 Ländern ausgestrahlt wurde. Heute ist er in die „G4“ übergegangen). In dem Beitrag wurden Fotos ihrer Schule gezeigt, die mich an die meines Heimatstädtchens Mechelen erinnerten. Auch die Fassade ihres Hauses wurde gezeigt. Als ich

einige Tage später durch ein Wohngebiet in meiner Nachbarschaft fuhr, wurde mir schlagartig klar, dass hier Gigabyte leben musste. Sieh an, ich hatte die Chance, sie zu demaskieren. Sarah Gordon war völlig aus dem Häuschen, als sie davon erfuhr. Sie bat mich gleich, den Kontakt zwischen ihr und Gigabyte herzustellen. Wir organisierten ein Treffen zwischen den beiden in einem Schloss in Luxemburg, unweit des Ortes, an dem auch eine EICAR-Konferenz (2004) stattfand. Es sorgte in der Antiviruswelt für einen riesen Wirbel, viele wollten wissen, mit wem sich Sarah traf und umso größer war das Erstaunen, als klar wurde, dass es sich um Gigabyte handelte. Peux á peux sickerte nämlich auch in der Antiviruswelt durch, dass es von Nutzen war, den Feind besser zu kennen und somit auch besser zu verstehen.

Fakt ist, dass diese Erkenntnis nur zögerlich angenommen wurde, was sich auch zeigte, als kurze Zeit später ein Virenschreiber einen Vortrag auf der Antiviruskonferenz Virus Bulletin halten sollte. Zugegeben, man lynchte ihn nicht, aber die Atmosphäre im Saal war äußerst feindlich, er wurde ständig mit Vorwürfen konfrontiert und sein Vortrag verlief alles andere als reibungslos.

http://www.springer.com/978-3-658-04760-3

Cybergefahr
Wie wir uns gegen Cyber-Crime und Online-Terror wehren können
Willems, E.
2015, XVIII, 188 S. 61 Abb., Softcover
ISBN: 978-3-658-04760-3