Eine Analyse von 33 Gigabyte gestohlener Keylogger-Daten

Thorsten Holz[1,2] Markus Engelberth[2] Felix C. Freiling[2]
[1]Secure Systems Lab, TU Wien [2]Universität Mannheim

Um an die sensiblen Daten der Opfer zu gelangen, verwenden Angreifer häufig *Keylogger*. Dies sind kleine Programme oder Browsererweiterungen, die die Tastaturanschläge an einem infizierten Rechner mitschneiden. Die so mitprotokollierten Daten werden in regelmäßigen Abständen an eine so genannte *Dropzone* geschickt. Dies ist ein Server im Internet, der die Daten aller Opfer eines Angreifers entgegennimmt und somit als zentraler Sammelpunkt dieser Daten dient. Auf diese Weise kann ein Angreifer bequem und anonymisiert auf die gesammelten Daten zugreifen, wodurch die Identifizierung des Täters schwierig wird.

Im Gegensatz zu anderen Studien, die nur auf das beobachtbare Handeln auf den Untergrundmarkt (etwa im IRC) fokussiert sind, präsentieren wir einen Überblick über die tatsächlich von Angreifern gestohlenen Güter.[1] Zu diesem Zweck haben wir zwei Keylogger-Familien näher analysiert – *Limbo*/*Nethell* und *ZeuS*/*Zbot*. Nach der Identifizierung der Dropzones mittels dynamischer Verhaltensanalyse, haben wir sieben Monate lang (April bis Oktober 2008) über 70 verschiedene Dropzones beobachtet. Häufig wurden bei den betrachteten Dropzones keine Authentifizierungsmethoden verwendet, so dass für den Zugriff auf die hinterlegten Daten lediglich die Adressen der Dropzones benötigt wurden. Insgesamt war es uns möglich, etwa 33 GB an Keylogger-Daten zu sammeln, die von über 173.000 kompromitierten Rechnern stammen.

Die Analyse der Keylogger-Daten erlaubt es uns, deren Gesamtwert auf dem Untergrundmarkt abzuschätzen: Jede einzelne auf einer Dropzone abgelegte Information besitzt einen speziellen Marktwert und stellt ein Handelsgut auf diesem Untergrundmarkt dar. Die für diese Abschätzung zugrundeliegenden Einzelpreise stammen aus einer Studie von Symantec[2], nach der die von uns gesichteten Güter einen Gesamtwert von $793.318 bis $16.604.605 haben. Diese große Spanne resultiert aus den teilweise sehr unterschiedlichen Einzelpreisen, die man auf dem Untergrundmarkt für bestimmte Güter bekommt. Zum Beispiel lassen sich Bankdaten laut der Symantec-Studie für $10 bis $1.000 verkaufen. Insgesamt konnten wir in den uns vorliegenden Keylogger-Daten 149.458 E-Mail-Passwörter, 78.359 vollständige Identitäten (bzgl. Sozialer Netzwerke), 10.775 Bankdaten, 7.105 Zugangsdaten für Auktionshäuser und 5.682 Kreditkartennummern identifizieren. Des Weiteren konnten wir beobachten, daß die Keylogger technisch immer ausgereifter sind und typischerweise so konfiguriert sind, dass sie aktiv werden, wenn die Opfer große Bankwebseiten besuchen.

[1]Th. Holz, M. Engelberth, F.C. Freiling: Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones. 14th European Symp. Research in Comp. Security (ESORICS), Sept. 2009.
[2]Symantec. Global Internet Security Threat Report, April 2008. Trends for July – December 07