

Projekteingabe

Titel: Malflare – dynamische trifft statische Codeanalyse

Studiengang: Informatik

Projektverfasser/Präsentator: Dominic Fischer und Daniel Jordi

Projektbetreuer: Dr. Endre Bangerter, M. Eng. Stefan Bühlmann

1. Projektbeschreibung

Die IT Security spielt mit der steigenden Vernetzung eine immer wichtigere Rolle. Internetkriminalität ist längst kein „Gentlemans Delikt“ mehr, sondern ist ein organisiertes Verbrechen welches Schätzungen zufolge jedes Jahr weltweit 82 Milliarden Euro Kosten verursacht.

In unserer Arbeit beschäftigten wir uns mit dem Reverse Engineering von Malware, also Schadprogramme wie Viren, Trojaner usw. welche die Hilfsmittel der Kriminellen sind. Beim Reverse Engineering werden zwei Methoden unterschieden: die statische und die dynamische Codeanalyse. Mit diesen Methoden kann die Funktionalität der Malware analysiert werden. Dies ist notwendig um schnellst möglich den verursachten Schaden rückgängig zu machen und/oder weiteren Schaden zu vermeiden. Die jeweiligen Analysetechniken weisen dabei Vor- und Nachteile auf. Die jeweiligen Nachteile werden durch die Programmierer der Malware schamlos ausgenutzt um die Zeit, bis ein Gegenmittel erstellt werden kann, zu verlängern: denn „Zeit ist Geld!“.

Schwerpunkt der Arbeit war das Zusammenführen der beiden Analysetechniken um die jeweiligen Nachteile aufzuheben und die Vorteile zu verstärken. Somit entstand ein mächtiges Werkzeug, welches das Analysieren vereinfacht und die Zeit verkürzt welche dazu benötigt wird um den Schaden rückgängig zu machen.

2. Innovation

Uns gelang die Verschmelzung der beiden Analysemethoden in einem bekannten und etablierten Reverse Engineering Werkzeug namens „IDA Pro“. Durch diese Zusammenführung werden die Nachteile der jeweiligen Analysetechnik aufgehoben. Neue Zusammenhänge werden aufgezeigt um somit die Analyse der Malware effizienter durchzuführen. Zusätzlich, nebst der Zusammenführung der Informationen, haben wir Funktionen implementiert welche den Anwender bei der Analyse von Malware weiter unterstützt. Diese Funktionen sind: Deadcode detektieren und kennzeichnen, Registeränderungen annotieren, Speicher rekonstruieren, Funktionsaufruf interpretieren, Programmschleifen detektieren und sicheres Code debuggen.

3. Clou

Die genannte Verschmelzung der beiden Analysetechniken gelang uns in einem auf dem Markt verfügbaren Programm namens *IDA Pro* (frei verfügbar). IDA Pro ist für die statische Analyse vorgesehen, jedoch konnten wir IDA Pro programmatisch mit den Informationen aus der dynamischen Codeanalyse erweitern.

Mit unserem Produkt haben wir den Grundstein für weitere Entwicklungen gelegt. Auf den nun zusammengeführten Daten können weitere hilfreiche Funktionen implementiert werden. Zudem kann unser System für andere Betriebssysteme wie Android, iOS usw. erweitert werden um auch spezifische Malware zu analysieren.

Unser in der Programmiersprache C++ umgesetzte Produkt gewann zudem den SWEN- Preis 2011: <http://www.swen-network.ch/swen-preis/preistrager-2011>

4. Kreativität

Da sich unser Produkt perfekt in die Bedienung des bestehenden Werkzeuges integriert, merkt der Bediener praktisch nicht, dass er unser Produkt verwendet. Lediglich die genannten, neuen Funktionalitäten lassen ihn stauen.

Weiter haben wir Funktionalitäten implementiert, welche es so noch nicht gegeben hat und für den sogenannten „Wow-Effekt“ sorgen.

5. Ausstrahlung

Unser Produkt ist in der Funktionalität umfangreich, die Bedienung jedoch ist sehr einfach und intuitiv. Die Chancen für eine Verbreitung in der Malware Community ist sehr gross, da unser Produkt am Hex-rays Plugin Contest 2011 (Hex-rays ist der Hersteller von IDA Pro) teilgenommen hat und sich somit bereits eine gewisse Bekanntheit verschafft hat. Das Feedback des Contests ist sehr positiv (siehe <http://www.hex-rays.com/contests/2011/index.shtml>) und hätte fast zum Sieg geführt.

Nun erhoffen wir uns eine schnelle Verbreitung und Ideen für Weiterentwicklungen. Ein weiterer positiver Aspekt ist die freie Verfügbarkeit unseres Produktes.

Unsere Idee ist sehr innovativ. Zum Zeitpunkt des Projektstartes waren keinerlei Vergleichbare Produkte auf dem Markt. Erst im Verlaufe der Arbeit kamen ähnliche, nicht so umfangreiche Produkte wie unseres auf den Markt.