ІПЗ-33\1 Гоша Давід Олександрович

Лабораторна №4

Назва програми	Пакувальник	Можливовсті пакувальника	Результати пакування		Працює(так/ні)	Програма ідентифікації пакувальника	Результат ідентифікації	Розпаковувальник	Результат розпакування	
			Обсяг	% збільш. зменьш					Обсяг	Працює(так/ні)
Delphi.exe 624 Kb	PECompact	Утиліта PECompact призначена для стиснення файлів .exe, .dll, .scr за допомогою численних алгоритмів	261 Kb	41.83%	так	PEiD	Аналіз проводиться по внутрішній та зовнішній базі сигнатур, є кілька рівнів сканування від швидкого до глибокого, можна обробляти цілі каталоги. Функціонал легко розширюється зовнішніми плагінами, сигнатури зберігаються в окремому текстовому файлі, тому ви легко можете додавати туди свої власні	PEiD	624 Kb	так

Delphi.exe 624 Kb	ASPack	Пакувальник ASPack простий у використанні і, завдяки потужному алгоритму, дозволяє досягти 40-70% стиснення для 32-бітових програм Windows. Файли, що підтримуються: .exe, .dll, .ocx, .dpl, .bpl (файли бібліотек Delphi)	251 Kb	40.22%	так	Detect it Easy (DiE)	Схожа на PEiD, але основний акцент робиться на власні евристичні аналізатори, а вже потім на сигнатурний аналіз. Також програма надає деякі корисні функції: перегляд імпорту, секцій, перегляд файлу в hex-режимі, дизассемблер, перегляд основних характеристик PE, отримання хеша MD5 та CRC-32. Функціонал розширюється за допомогою плагінів. Завантажити DiE можна	DiE	0	ні
Delphi.exe 624 Kb	UpxVis	UPX (The Ultimate Packer for eXecutables) - швидкий пакувальник, який працює в консольному режимі і дозволяє досягти високих коефіцієнтів стиснення. Також може виконувати декомпресію. Формати файлів, що підтримуються: exe, sys, com, pe (Win32), 386 (Linux) та ін.	253 Kb	40.54%	так	ExeInfo PE	Також дуже схожа на PEiD, остання версія 0.0.3.3 від квітня 2013 року. Сигнатури вбудовані (470 штук) і не розширюються. У програмі є цікава функція: якщо протектор визначений, вона дає інформацію, з якого інструменту його можна спробувати распаковать. Для новачків ця інформація буде дуже корисною	ExeInfo PE	0	ні
Main.py 4 mb	PyInstaller	При генерації файлу створюється архів, який містить віртуальну машину Python і всі необхідні бібліотеки. Сам вихідний код програми при цьому перетворюється на байт код і його не можна дезасемблювати.	5 mb	125%	так	ExeScan	Колишня приватна утиліта від крякерської команди SnD. Працює зі своїм форматом зовнішніх сигнатур та своїм же форматом плагінів. Мабуть через таку всебічну закритість цей аналізатор не отримав широкого визнання, хоча задум дуже хороший.	ExeScan	2.78 mb	так

Delphi.exe 624 Kb	UPX	UPX — це вдосконалений компресор виконуваних файлів. UPX зазвичай зменшує розмір файлів програм і DLL приблизно на 50%-70%, таким чином зменшуючи дисковий простір, час завантаження мережі, час завантаження та інші витрати на розповсюдження та зберігання.	311	50.45%	так	Pe-Scan	Це евристичний та сигнатурний аналізатор виконуваних файлів, розпакувальник деяких пакерів, динамічний пошук OEP. Крім перелічених інструментів у Pe-Scan є унікальний ймовірнісний аналізатор для незнайомих пакувальників та шифрувальників файлів (кнопка "adv.scan").	Pe-Scan	624 Kb	так

Висновки

Пакувальник UPX з оболонкою UpxVis показав найкраще стиснення виконуваних файлів (.exe). Враховуючи те, що програма розповсюджується безкоштовно, можна сказати, що для пакування "екзешників" доцільніше застосовувати саме її. Якщо UPX щось не зможе зробити добре, він вам про це неодмінно повідомить. Для стиснення dll та файлів з оверлеєм (не настановних!) краще використовувати ASPack, т.к. він працює надійніше та швидше. Я швидше за все виберу саме його. А PECompact підкуповує лише можливістю вибору кодеків, з якими можна поекспериментувати на дозвіллі. Він стискає майже так, як і ASPack, тільки іноді витрачає на це більше часу.