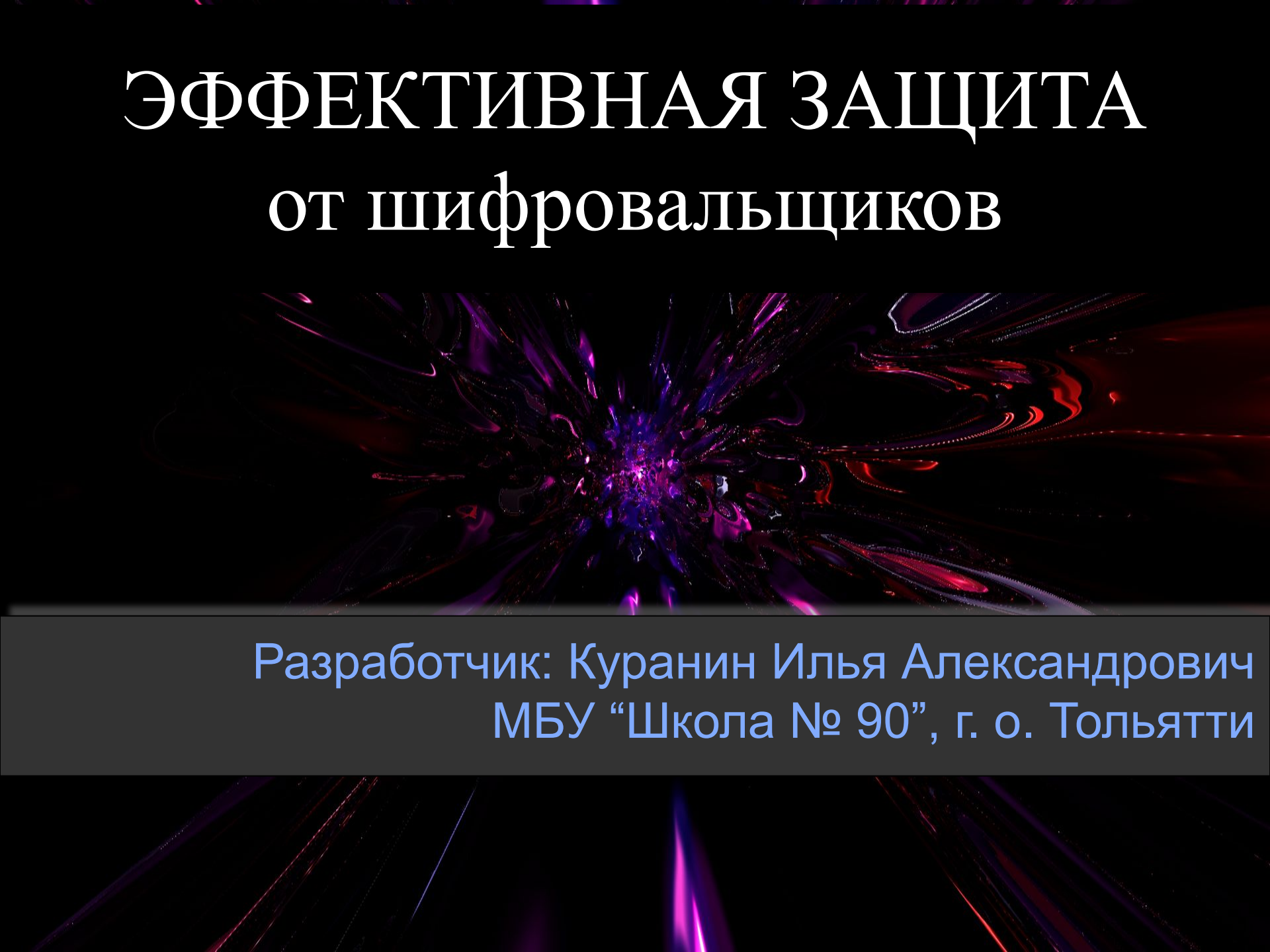


ЭФФЕКТИВНАЯ ЗАЩИТА от шифровальщиков



Разработчик: Куранин Илья Александрович
МБУ “Школа № 90”, г. о. Тольятти

- **Актуальность:** в настоящее время широко распространены различного рода троянские программы-вымогатели (Ransomware), среди которых наиболее часто встречаются шифровальщики, блокирующие файлы пользователя и требующие за восстановление данных выкуп. Таким образом, вышеперечисленные угрозы могут нанести значительный ущерб, вследствие чего появилась идея разработать приложение, основная цель которого – защитить компьютер от хакерских атак и предотвратить заражение системы.
- **Объектом исследований** является защита от троянских программ-шифровальщиков.
- **Предметом исследований** – антивирусные утилиты.
- **Цель** – создание двух антивирусных утилит для очистки компьютера от уже присутствующих на территории системы угроз, а также для защиты от нового, еще неизвестного вредоносного и потенциально опасного программного обеспечения.

Главные задачи

- Провести анализ поведения вредоносного ПО класса Ransomware для дальнейшего создания средств защиты
- Использовать “облачные” определения, т. е. анализ еще неизвестных утилитами файлов на собственном сервере
- Разработать эвристический анализатор угроз по характерному для них поведению
- Обеспечивать пользователю безопасную рабочую среду
- Использовать распределение нагрузки на центральный процессор для комфортной работы



Языки программирования:

Microsoft Visual Studio:

Basic

Visual Basic Script

Microsoft Visual Fox Pro

Command Processor Windows
(CMD, BAT)

Исправление кода:

Pe Explorer

Тестирование приложения

(виртуальные среды):

Oracle VirtualBox

VmWare Workstation

Сайты-архивы вирусов:

VirusShare.com

VirusSign.com

Malc0de.com

MalShare.com

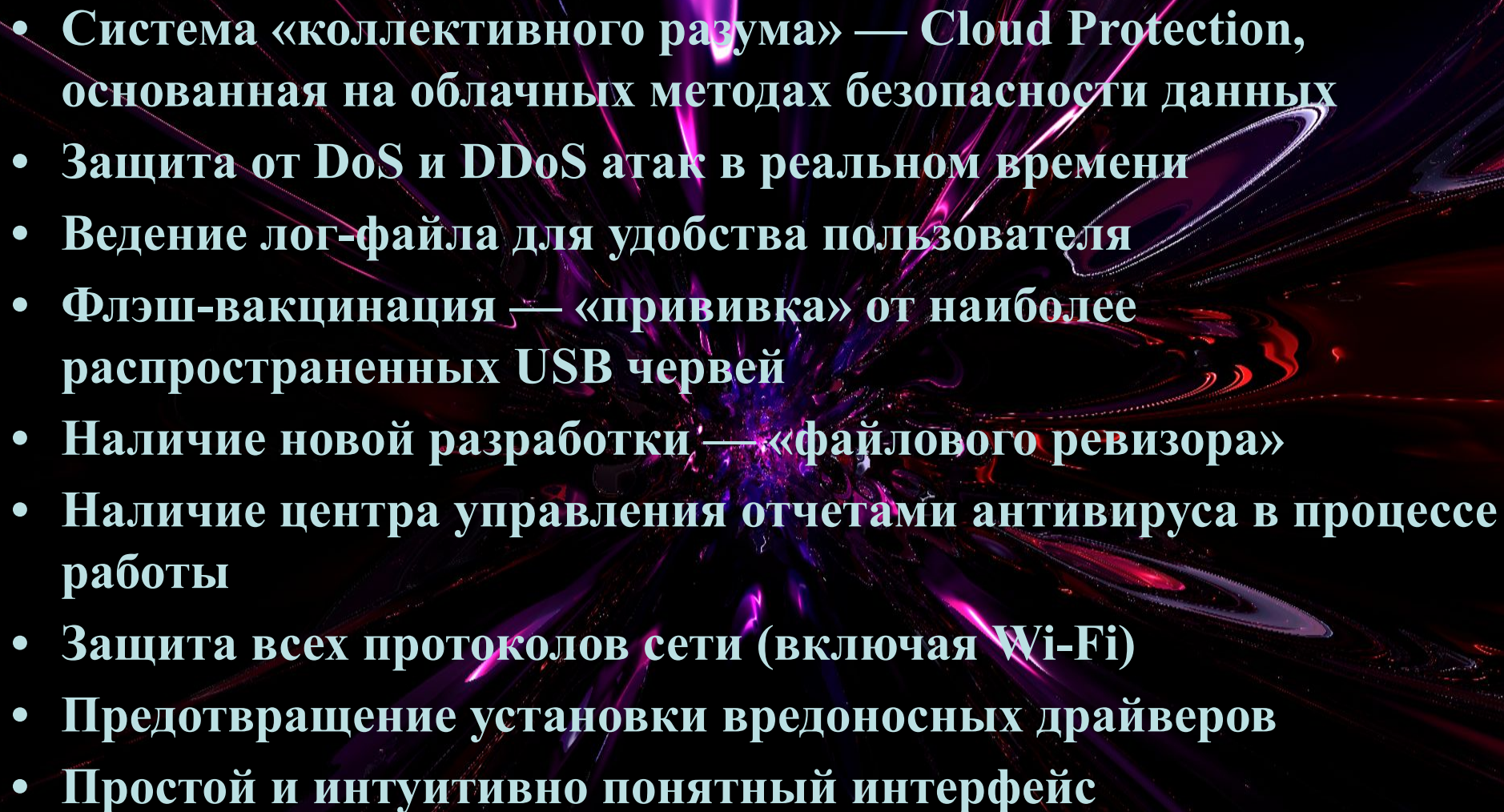
VxVault.net

Схема работы компонентов Kurantin Anti-Ransomware:



Технические характеристики

- Базовая и эвристическая защиты в режиме реального времени
- Защита и оптимизация реестра системы в режиме реального времени
- Защита USB/CD/DVD съемных носителей от заражения autorun-зловредами
- Защита Интернет-соединения
- Защита от фишинговых, мошеннических и вредоносных веб-ресурсов
- HIPS (поведенческий) анализатор
- Возможность использования на серверах и в корпорациях
- Защита от подмены системных файлов
- Комплексная защита автозагрузки системы

- 
- Система «коллективного разума» — **Cloud Protection**, основанная на облачных методах безопасности данных
 - Защита от **DoS** и **DDoS** атак в реальном времени
 - Ведение лог-файла для удобства пользователя
 - Флэш-вакцинация — «прививка» от наиболее распространенных **USB** червей
 - Наличие новой разработки — «**файлового ревизора**»
 - Наличие центра управления отчетами антивируса в процессе работы
 - Защита всех протоколов сети (включая **Wi-Fi**)
 - Предотвращение установки вредоносных драйверов
 - Простой и интуитивно понятный интерфейс

Механизм заражения исполняемых файлов. Изменения в структуре исполняемого файла после заражения

Схема работы исполняемого файла без заражения

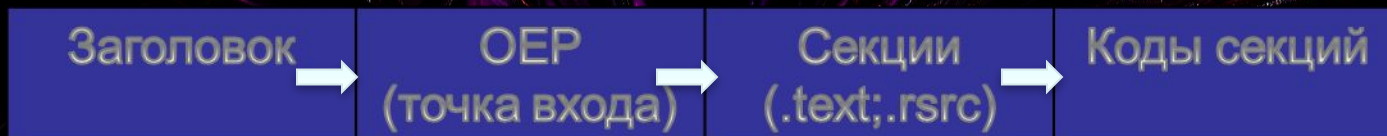
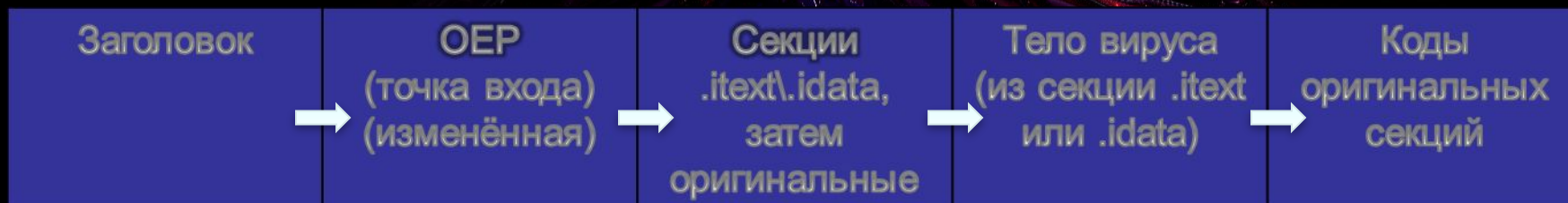
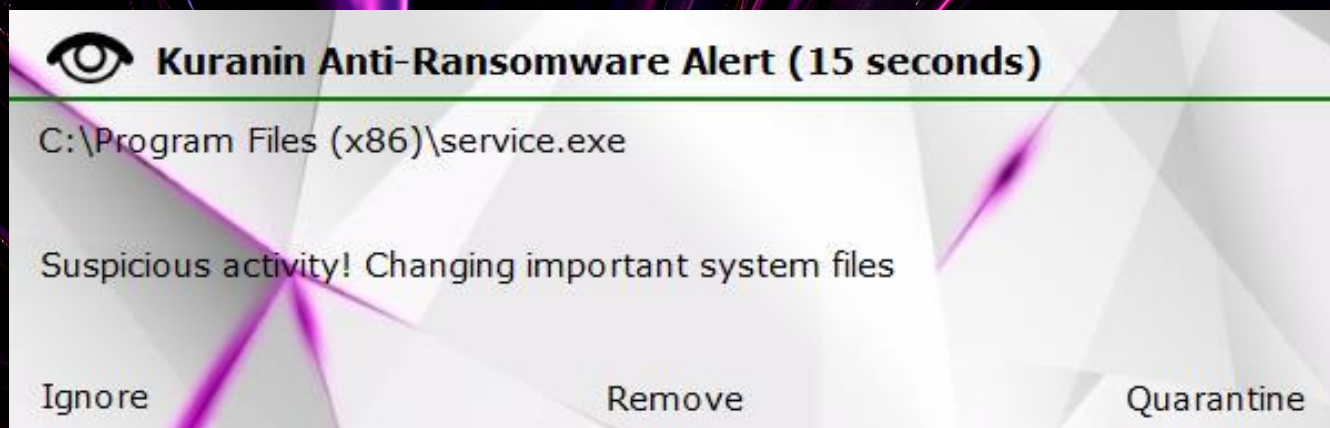


Схема работы исполняемого файла после заражения



При обнаружении вируса или подозрительной программы пользователь получает сообщение в виде окна обнаружения, звукового сигнала и отсчета времени. По истечении 15 секунд объект перемещается в карантин



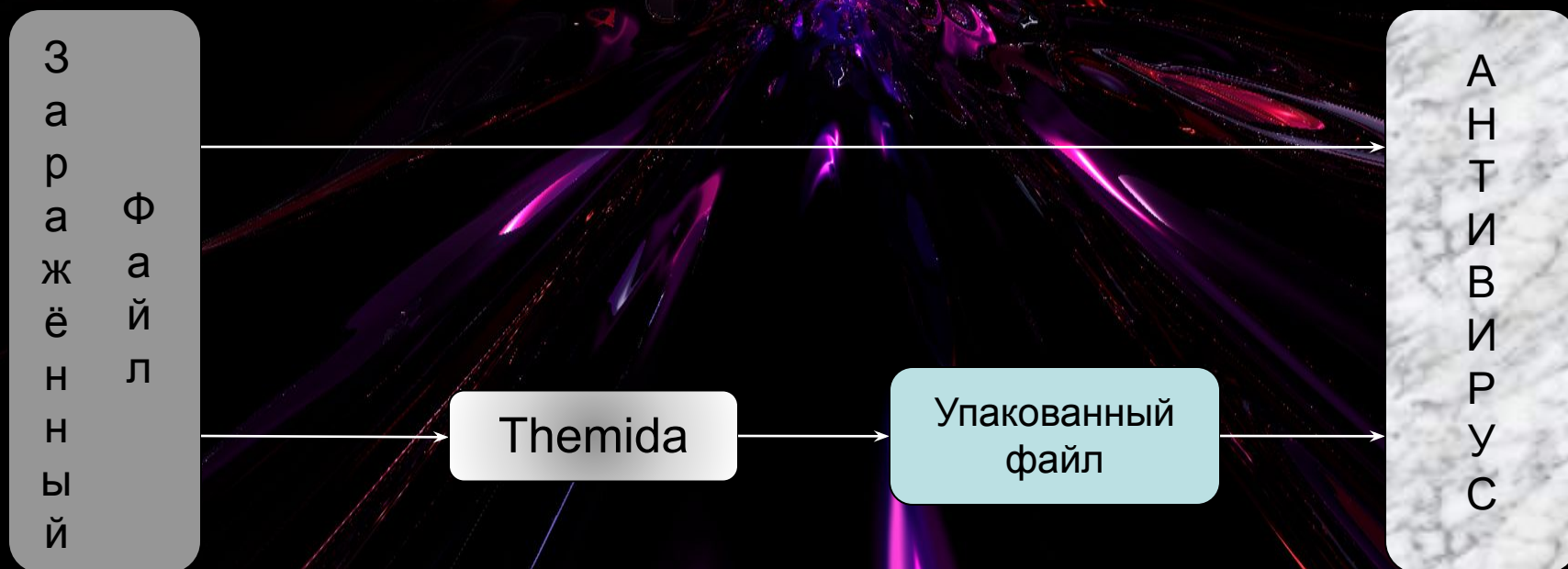
Новые
антивирусные
базы, а также
исправления
модулей
программы
выпускаются
один раз в день

Один из алгоритмов обнаружения Ransomware



Сравнение способности антивирусных утилит находить Ransomware без с протектором Themida:

	WinPatrol	BitDefender	CyberSight	ZoneAlarm	NoMoreCry	360 Protector	Kuranin Anti-Ransom
Ransom.Jigsaw	Обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен
Ransom.BadRabbit	Обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен
WannaCry 2.0	Обнаружен	Обнаружен	Не обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен
CryptoManiak	Не обнаружен	Обнаружен	Обнаружен	Не обнаружен	Не обнаружен	Не обнаружен	Обнаружен
Godra Ransomware	Обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен	Обнаружен



Результаты синтетического теста Fortinet CheckMetal

Kuranin Anti-Ransomware

- ✓ Вымогатели
- ✗ Кража личных данных / фишинг
- ✓ Уязвимость Zero Day
- ✓ Болезни Инфекции
- ✓ Атака браузера
- ✓ Использование анонимайзера
- ✓ Чувствительная утечка данных

✓ Безопасный ✗ уязвимый

Kaspersky Internet Security

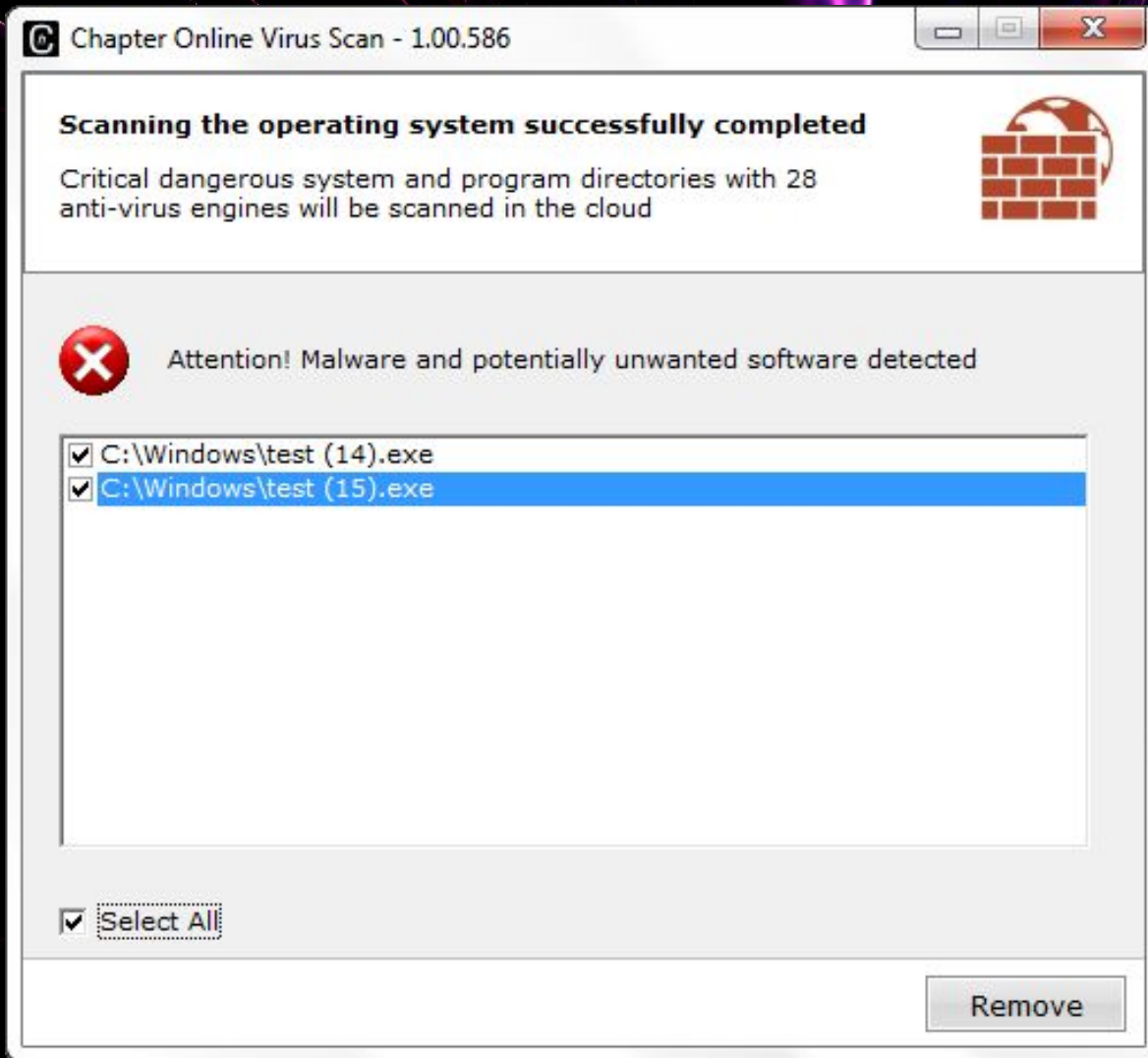
- ✓ Вымогатели
- ✗ Кража личных данных / фишинг
- ✗ Уязвимость Zero Day
- ✗ Болезни Инфекции
- ✗ Атака браузера
- ✗ Использование анонимайзера
- ✗ Чувствительная утечка данных

Chapter Cloud Virus Scan

Облачный антивирусный сканер, работающий на 28 антивирусных движателях

- Проверка критических директорий Windows, System32, Wbem и временных папок на наличие неизвестных исполняемых файлов
- Отсеивание безопасных образцов по белому списку с использованием контрольной MD5 хеш-суммы
- Загрузка неизвестных объектов на контрольный сервер
- Специальный комплекс проверяет файлы на наличие вредоносного кода
- Объекты запускаются в песочнице Sandbox, происходит анализ поведения в памяти
- Ответ от сервера о степени риска файлов

Обнаружение вредоносных файлов облачным сканером:



Минимальные системные требования:

ОС: Windows с правами администратора;

RAM: 512 Мб;

Процессор: 300 MHz и выше;

Не менее 50Мб свободного места;

Интернет-соединение со скоростью не менее 500 КБ/с

Манипуляторы:

мышь

Часть кода антивирусной программы Kuranin Anti-Ransomware:

<...>

On Error Resume Next

ZwSetInformationProcess GetCurrentProcess(), &H21&, VarPtr(&H8000F129), &H4&

If App.PrevInstance = True Then End

Me.Hide

ChDir App.Path

CurDir App.Path

Text1 = ""

Form3.Show

Dim hSnapShot As Long

Dim uProcess As PROCESSENTRY32

Dim r As Long

hSnapShot = CreateToolhelpSnapshot(TH32CS_SNAPPROCESS, 0&)

If hSnapShot = 0 Then

Exit Sub

End If

uProcess.dwSize = Len(uProcess)

r = ProcessFirst(hSnapShot, uProcess)

Do While r

Text1 = Text1 + " " + uProcess.szExeFile

r = ProcessNext(hSnapShot, uProcess)

Loop

Call CloseHandle(hSnapShot)

Randomize

(2)

If FileLen(Environ("windir") & "\system32\MSCOMCTL.OCX") = 0 Then FileCopy App.Path & "MSCOMCTL.OCX", Environ("windir") & "\system32\MSCOMCTL.OCX"

(3)

If Not Command Like "*" /Start=*" & Date & "*" Then End

Награды и оценки пользователей Chapter Cloud Virus Scan

Chapter Cloud Virus Scan 5.181.023

Описание

СКАЧАТЬ (640 Кб)

Скриншоты (3)

Статистика

Отзывы (3)

Chapter Cloud Virus Scanner - это легкий портативный антивирусный сканер, работающий в облаке и совместимый со сторонними защитными программами. Принцип работы приложения основан на системе "коллективного разума":

- Выполняется построение списка не находящихся в белом списке исполняемых файлов из временных папок и критических директорий Windows, System32, Wbem.
- Объекты загружаются на сервер компании и проверяются с помощью 28 антивирусных двигателей.
- Код файлов анализируется на предмет подозрительного поведения.
- Выносятся вердикт касательно безопасности объектов.

Оцените программу!

4.70 из 5, всего оценок - 63



Программы » Безопасность » Антивирусы » Chapter Cloud Virus Scan скачать бесплатно

Chapter Cloud Virus Scan 1.00.56

Скачать



Рейтинг 5.0 из 5 Оценок: 4

Лицензия: Бесплатно (Freeware)

Язык: Английский

ОС: Windows XP, Vista, 7, 8, 10

Разработчик: Ilya Kuranin

Закачек: 153

Обзор программы

Chapter Cloud Virus Scan - 1.00.586

Chapter Techno

SOFTPORTAL
www.softportal.com

Показов 18/1851

Закачек 4/326

Голосов 63

Отзывов 3

★★★★★ 4.7

Спасибо за внимание!