

Dr.Web FixIt!: практический опыт расследования кибер-инцидентов глазами антивирусной компании



Василий Севостьянов

Руководитель отдела по
Техническому сопровождению
продаж
ООО «Доктор Веб»



Немного истории

Ликвидация последствий кибер-инцидентов:

- Недостаток квалификации пользователей
- Удаленный сбор информации для расследования
- Удаленное лечение произвольных угроз в неизвестных неконтролируемых условиях



Собираемая информация

- Общая информация о системе
- Системные журналы (event logs), логи антивируса
- Установленное ПО, обновления системы, запущенные процессы, драйверы, сервисы, активные сетевые соединения и пр.
- Основные ветки реестра системы
- Загрузочные сектора дисков



Сервис FixIt!

1. Задача на анализ, в которой генерируется ссылка на индивидуальную сборку утилиты FixIt! для передачи клиенту
2. Утилита формирует отчет
3. Анализ отчета в сервисе, формирование лечащей утилиты
4. Лечение, повторный сбор отчета
5. Повтор 3-4 до устранения последствий инцидента



Задача на анализ

 **Dr.WEB** FixIt!

Задачи 

Новая задача 

Открыто 42 Закрыто 0 Лимит Безлимитно Доступно Безлимитно





Генерация утилиты



[← Назад](#) / Workstation 001

Workstation 001

Создатель	Vasiliy Sevostyanov	Дата создания	15.10.2021 12:22
Отчеты	—	Последнее изменение	15.10.2021 13:19

[+ Заметка](#)

Отчетов пока нет

Создайте утилиту FixIt! и отправьте ее пользователю, чтобы получить отчет. Утилита создаст отчет после проверки компьютера пользователя. Если отчет не загрузится автоматически, загрузите его вручную.

[✎ Создать](#) [📄 Загрузить отчет](#)

Утилита FixIt!

▼ Настройки

 Команды

 Создать

☒ Автоматически загружать отчеты:

В эту задачу

На URL

https://

☒ Отправлять данные об обнаруженных угрозах и о примененных действиях в «Доктор Веб»

☒ Использовать Dr.Web Cloud

☒ Собирать подозрительные файлы

☐ Не использовать сигнатурный анализ



Анализ отчета

Dr.WEB FixIt!

Пространство

Фильтры

Профиль

Об отчете

Данные

Система

Процессы

Драйверы

Службы

Сеть

Автозапуск

Планировщик заданий

Веб-браузеры

Журнал событий

Реестр

Файловая система

Поиск и анализ

Утилита FixIt!

Файлы

Назад / Report 1633884563.721784

Поиск и анализ

Готовые фильтры

Новый фильтр

Выбранные действия

Metawave detects

Microsoft Defender (t...

Microsoft defender (t...

Certificates detects

Signature detects

Non-signature detects

Cloud URL detects

Signature detects

Действие ▾	Тип ⚡	Путь ⚡	Угроза ⚡	Тип ⚡
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware
☐ None ▾	Сигнатурны...	> C:\Program Files (x86)\Lavasoft\Web Companion\Ap...	Program.Unwanted.4990	riskware



Лечащая утилита

Пространство Фильтры Профиль

Об отчете

Данные ^

Система

Процессы

Драйверы

Службы

Сеть

Автозапуск

Планировщик заданий

Веб-браузеры

Журнал событий

Реестр

Файловая система

Поиск и анализ

Утилита FixIt!

Файлы

← Назад / Report 1633884563.721784

Утилита FixIt!

> Настройки

Команды Создать

1 cure-file "C:\\Users\\pasho\\AppData\\Local\\Host App Service\\Engine\\HostAppService.exe"

2 cure-file "C:\\WINDOWS\\TEMP\\wctmp_157594198\\WcInstaller.exe"

3 cure-file "C:\\Program Files (x86)\\Lavasoft\\Web Companion\\Application\\Lavasoft.WCAssistant.WinService.exe"

4 cure-file "C:\\Program Files (x86)\\Lavasoft\\Web Companion\\Application\\WebCompanion.exe"

5 cure-file "C:\\Program Files (x86)\\Lavasoft\\Web Companion\\Service\\x64\\DCIService.exe"

6 fs-remove "C:\\Program Files (x86)\\Lavasoft\\Web Companion"



Основные возможности

- Антируткит – лечение системных объектов и элементов реестра
- Сигнатурные детекты – лечение объектов (файловые объекты, элементы реестра, WMI, и пр.) и обезвреживание процессов
- Файловая система (базовые операции, очистка ACL и ADS)
- Процессы (запуск, завершение, заморозка)



Основные возможности

- Службы (запуск, завершение, удаление, передача управляющих кодов)
- Планировщик заданий (запуск, удаление задач)
- WMI providers
- Файл HOSTS
- Расширения и конфигурация браузеров
- Сбор дополнительной информации



Поиск и аналитика

- Предсозданные фильтры
 - Общие (уязвимые драйверы, активные RDP сессии, скриптовые интерпретаторы, неподписанные исполняемые файлы, файлы с необычными сертификатами подписи, руткиты, известные утилиты удаленного доступа, хакерские утилиты и пр.)
 - Обновления ОС (MS17-010, BlueKeep, PrintNightmare и пр.)
 - Сигнатурные детекты антивируса, несигнатурные детекты, прочие детекты
 - Индикаторы известных семейств ВПО
- Персональные фильтры



Общая последовательность

- Анализ содержимого файловой системы
- Системный реестр
- Журнал событий (event log) системный, антивируса
- Сетевые настройки
- Запущенные процессы
- Информация о системе



Кейс #1

APT backdoor

- Предыстория
 - Обращение от клиента: «Не определяется вирус. Постоянно появляется в папке C:\ProgramData\SymantecAV. Содержимое прилагаю».



Ищем APT backdoor

Dr.WEB FixIt!

ManagementFiltersProfile

AboutDataSystemProcessesDriversServicesNetworkStartupsTask schedulerEvent logRegistryFile systemSearch and analyzeFixIt! toolFiles

Back / Report 1634115106.069531

Search and analyze

Defined filtersNew filterSelected actions

Internet downloaded ...Exploitable driversActive RDP sessionsScripted engine inter...New executables filesSecurity providers pr...Unsigned untrusted e...

DLL Hijacking w/ trusted process

Action	Type	Path	hash.sha256	arkstatus.file
☐ None	Files	C:\Windows\EH5rv.exe	> 81698c9d6e69506637208ca564b14b7febbfe4efbc574c...	[db_cert_white_list.signed,pe32]
☐ None	Files	C:\Windows\System32\oci.dll	> e7b50c499cd9ec8efa9150aa8d6483da5ec344c34c4fd1...	[unsigned,pe64,dll]
☐ None	Files	> C:\microsoft\temp\networks\connections\pbksn4\wind...	> f9ebf6aeb3f0fb0c29bd8f3d652476cd1fe8bd9a0c11cb1...	[db_cert_white_list.signed,pe32]
☐ None	Files	C:\Windows\TEMP\tsumk.exe	> f9ebf6aeb3f0fb0c29bd8f3d652476cd1fe8bd9a0c11cb1...	[db_cert_white_list.signed,pe32]
☐ None	Files	C:\Windows\IME\tsmk.exe	> f9ebf6aeb3f0fb0c29bd8f3d652476cd1fe8bd9a0c11cb1...	[db_cert_white_list.signed,pe32]
☐ None	Files	C:\windows\inf\svcs\cy.exe	> f9ebf6aeb3f0fb0c29bd8f3d652476cd1fe8bd9a0c11cb1...	[db_cert_white_list.signed,pe32]
☐	Loaded mod...	C:\Windows\System32\oci.dll	—	—

Collapse

© Doctor Web, 1992–2021

About FixIt!About usPrivacy policySupportEnglish



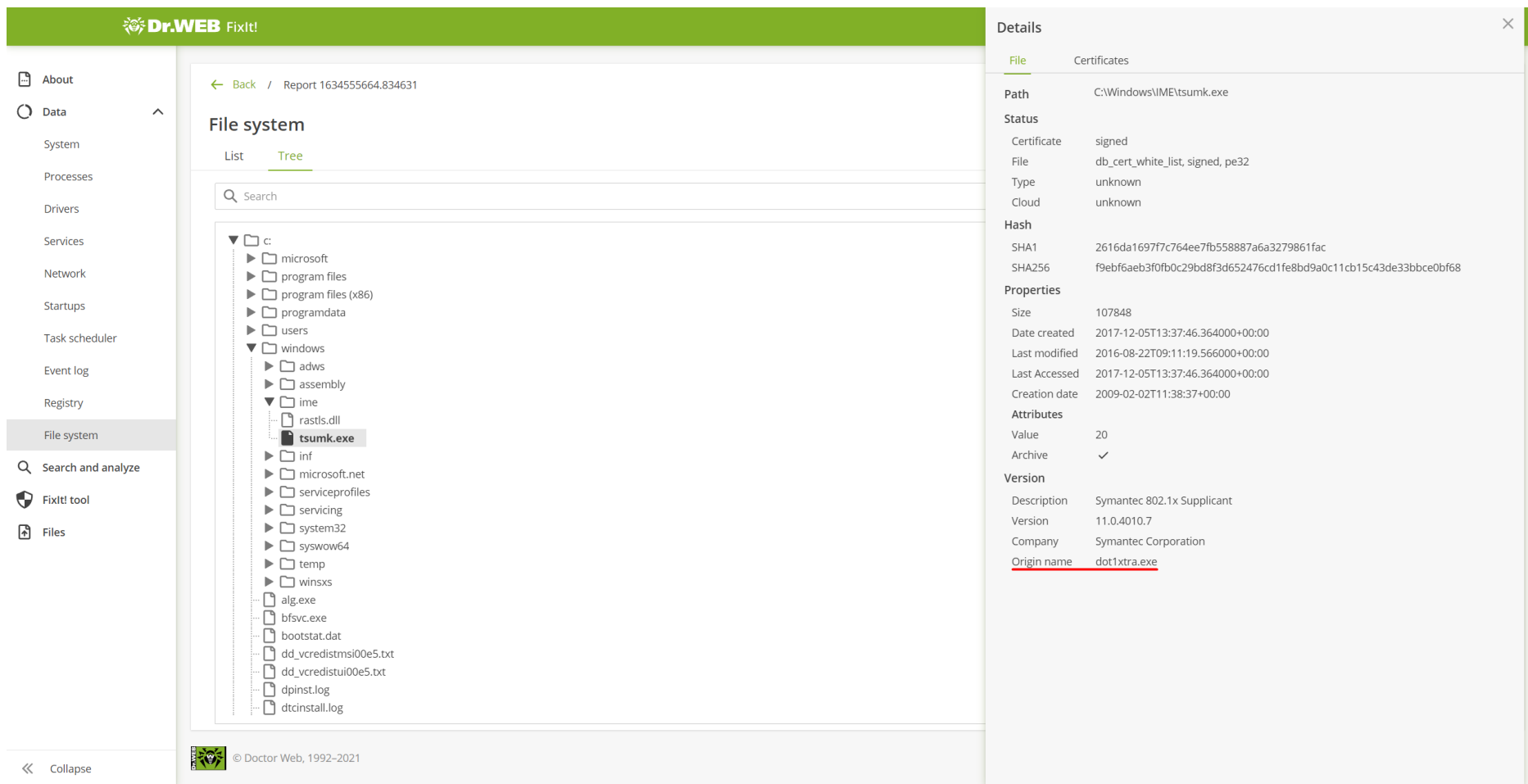
© ООО «Доктор Веб», 2021

www.антивирус.рф

www.drweb.ru



Ищем APT backdoor



The screenshot displays the Dr.Web FixIt! application interface. On the left is a sidebar with navigation options: About, Data, System, Processes, Drivers, Services, Network, Startups, Task scheduler, Event log, Registry, File system (selected), Search and analyze, FixIt! tool, and Files. The main area shows a file system tree for 'Report 1634555664.834631'. The tree is expanded to show the 'c:\windows\ime\rastls.dll\tsumk.exe' file. The right pane shows details for this file, including its path, status, certificate information, hash (SHA1 and SHA256), properties (size, creation/modification/access dates, creation date), attributes (value, archive), and version (description, version number, company). The 'Origin name' is listed as 'dot1xtra.exe'.

File system

Back / Report 1634555664.834631

List Tree

Search

c:\

- microsoft
- program files
- program files (x86)
- programdata
- users
- windows
 - adws
 - assembly
 - ime
 - rastls.dll
 - tsumk.exe**
 - inf
 - microsoft.net
 - serviceprofiles
 - servicing
 - system32
 - syswow64
 - temp
 - winsxs
- alg.exe
- bfsvc.exe
- bootstat.dat
- dd_vcredistmsi00e5.txt
- dd_vcredistui00e5.txt
- dpinst.log
- dtcinstall.log

Details

File Certificates

Path C:\Windows\IME\tsumk.exe

Status

Certificate signed

File db_cert_white_list, signed, pe32

Type unknown

Cloud unknown

Hash

SHA1 2616da1697f7c764ee7fb558887a6a3279861fac

SHA256 f9ebf6aeb3f0fb0c29bd8f3d652476cd1fe8bd9a0c11cb15c43de33bbce0bf68

Properties

Size 107848

Date created 2017-12-05T13:37:46.364000+00:00

Last modified 2016-08-22T09:11:19.566000+00:00

Last Accessed 2017-12-05T13:37:46.364000+00:00

Creation date 2009-02-02T11:38:37+00:00

Attributes

Value 20

Archive ✓

Version

Description Symantec 802.1x Supplicant

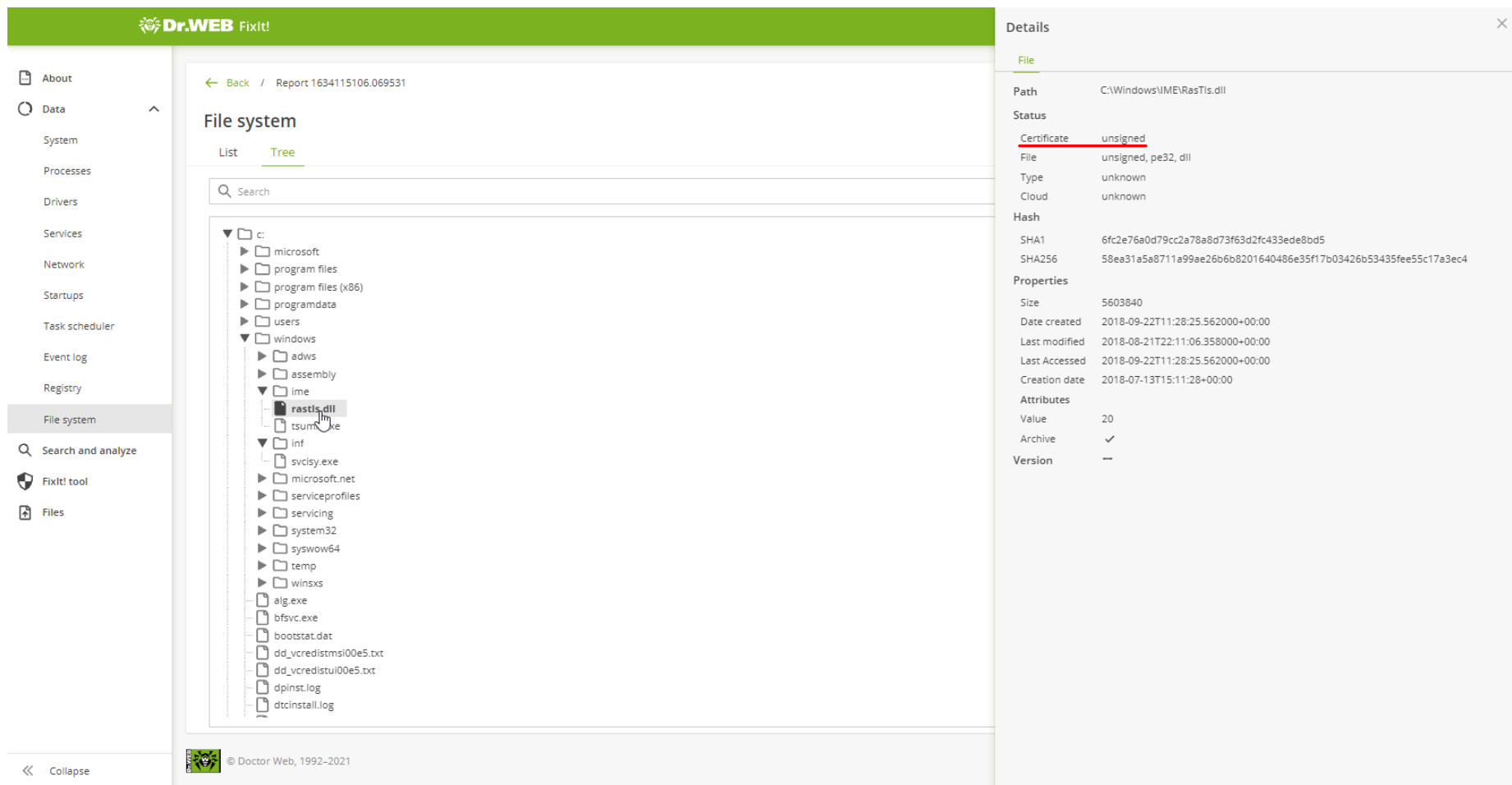
Version 11.0.4010.7

Company Symantec Corporation

Origin name dot1xtra.exe



Ищем APT backdoor

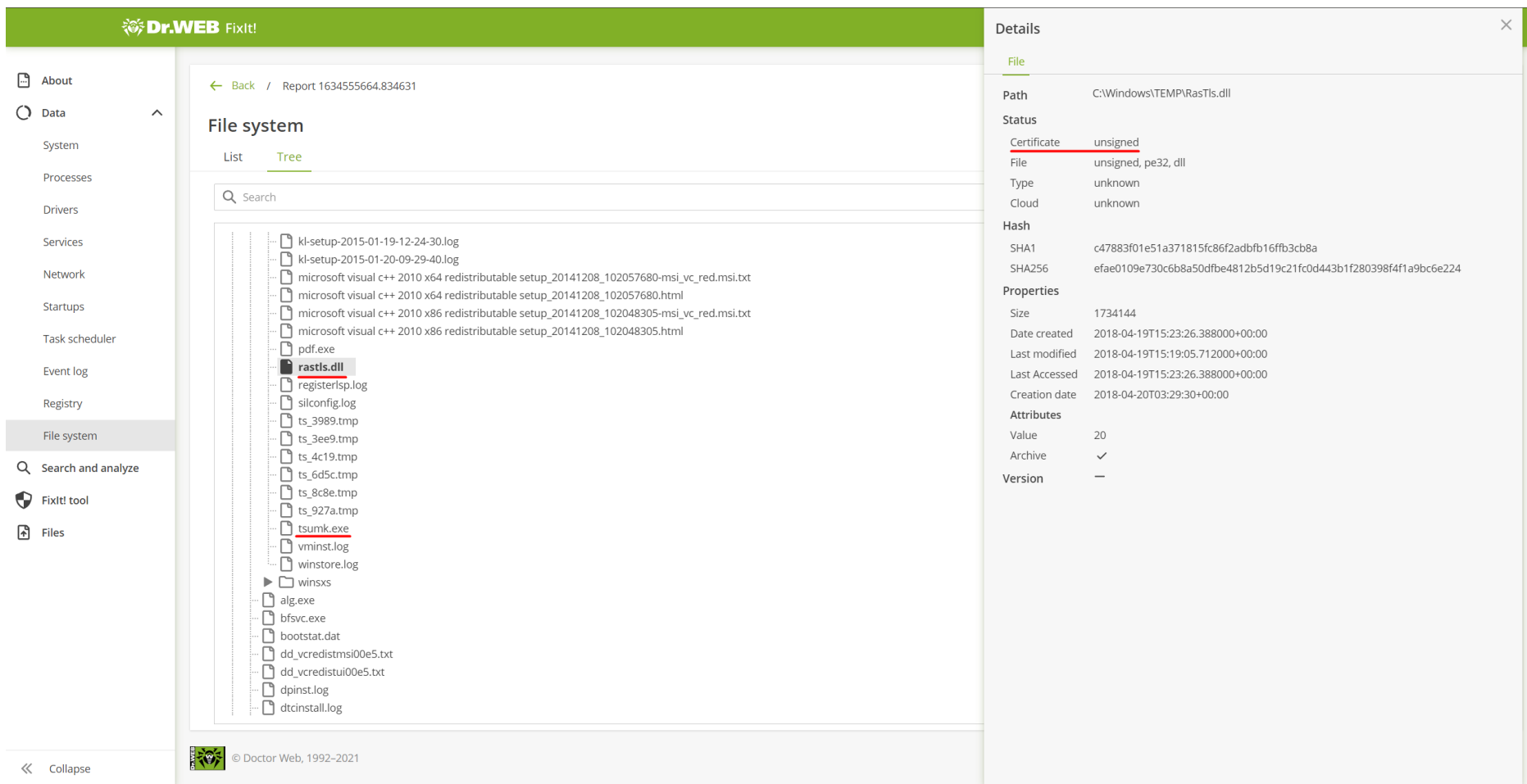


The screenshot shows the Dr.Web FixIt! application interface. On the left is a sidebar with navigation options: About, Data, System, Processes, Drivers, Services, Network, Startups, Task scheduler, Event log, Registry, File system (selected), Search and analyze, FixIt! tool, and Files. The main window displays the 'File system' view for a specific report (1634115106.069531). It shows a tree view of the file system with 'rastls.dll' highlighted under the 'ime' folder in the 'windows' directory. A 'Details' pane on the right provides information about the selected file:

File	
Path	C:\Windows\IME\RasTls.dll
Status	
Certificate	unsigned
File	unsigned, pe32, dll
Type	unknown
Cloud	unknown
Hash	
SHA1	6fc2e76a0d79cc2a78a8d73f63d2fc433ede8bd5
SHA256	58ea31a5a8711a99ae26b6b8201640486e35f17b03426b53435fee55c17a3ec4
Properties	
Size	5603840
Date created	2018-09-22T11:28:25.562000+00:00
Last modified	2018-08-21T22:11:06.358000+00:00
Last Accessed	2018-09-22T11:28:25.562000+00:00
Creation date	2018-07-13T15:11:28+00:00
Attributes	
Value	20
Archive	✓
Version	---



Ищем APT backdoor



The screenshot shows the Dr.Web FixIt! application interface. The left sidebar contains navigation options: About, Data, System, Processes, Drivers, Services, Network, Startups, Task scheduler, Event log, Registry, File system (selected), Search and analyze, FixIt! tool, and Files. The main area displays a file system tree for a specific report (1634555664.834631). The tree shows various files and folders, with **rastls.dll** highlighted. The right pane shows details for the selected file, including its path, status, certificate, file type, cloud status, hash (SHA1 and SHA256), properties (size, date created, last modified, last accessed, creation date), attributes (value, archive, version), and version.

File system

← Back / Report 1634555664.834631

List Tree

Search

- kl-setup-2015-01-19-12-24-30.log
- kl-setup-2015-01-20-09-29-40.log
- microsoft visual c++ 2010 x64 redistributable setup_20141208_102057680-msi_vc_red.msi.txt
- microsoft visual c++ 2010 x64 redistributable setup_20141208_102057680.html
- microsoft visual c++ 2010 x86 redistributable setup_20141208_102048305-msi_vc_red.msi.txt
- microsoft visual c++ 2010 x86 redistributable setup_20141208_102048305.html
- pdf.exe
- rastls.dll**
- registerlsp.log
- silconfig.log
- ts_3989.tmp
- ts_3ee9.tmp
- ts_4c19.tmp
- ts_6d5c.tmp
- ts_8c8e.tmp
- ts_927a.tmp
- tsumk.exe**
- vminst.log
- winstore.log
- winsxs
 - alg.exe
 - bfsvc.exe
 - bootstat.dat
 - dd_vc_redistmsi00e5.txt
 - dd_vc_redistui00e5.txt
 - dpinst.log
 - dtcinstall.log

Details

File

Path C:\Windows\TEMP\Rastls.dll

Status

Certificate unsigned

File unsigned, pe32, dll

Type unknown

Cloud unknown

Hash

SHA1 c47883f01e51a371815fc86f2adbfb16ffb3cb8a

SHA256 efae0109e730c6b8a50dfbe4812b5d19c21fc0d443b1f280398f4f1a9bc6e224

Properties

Size 1734144

Date created 2018-04-19T15:23:26.388000+00:00

Last modified 2018-04-19T15:19:05.712000+00:00

Last Accessed 2018-04-19T15:23:26.388000+00:00

Creation date 2018-04-20T03:29:30+00:00

Attributes

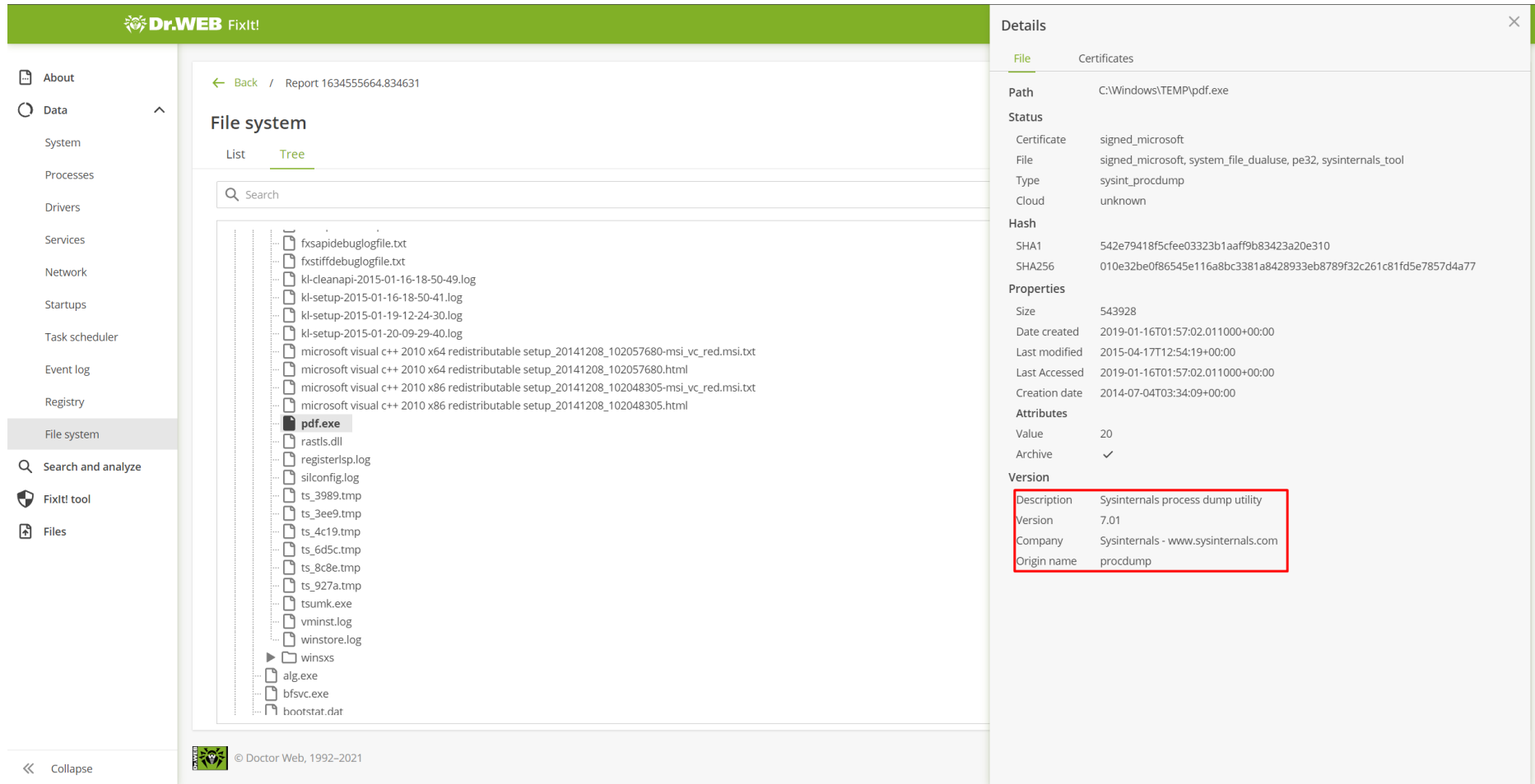
Value 20

Archive ✓

Version —



Ищем APT backdoor

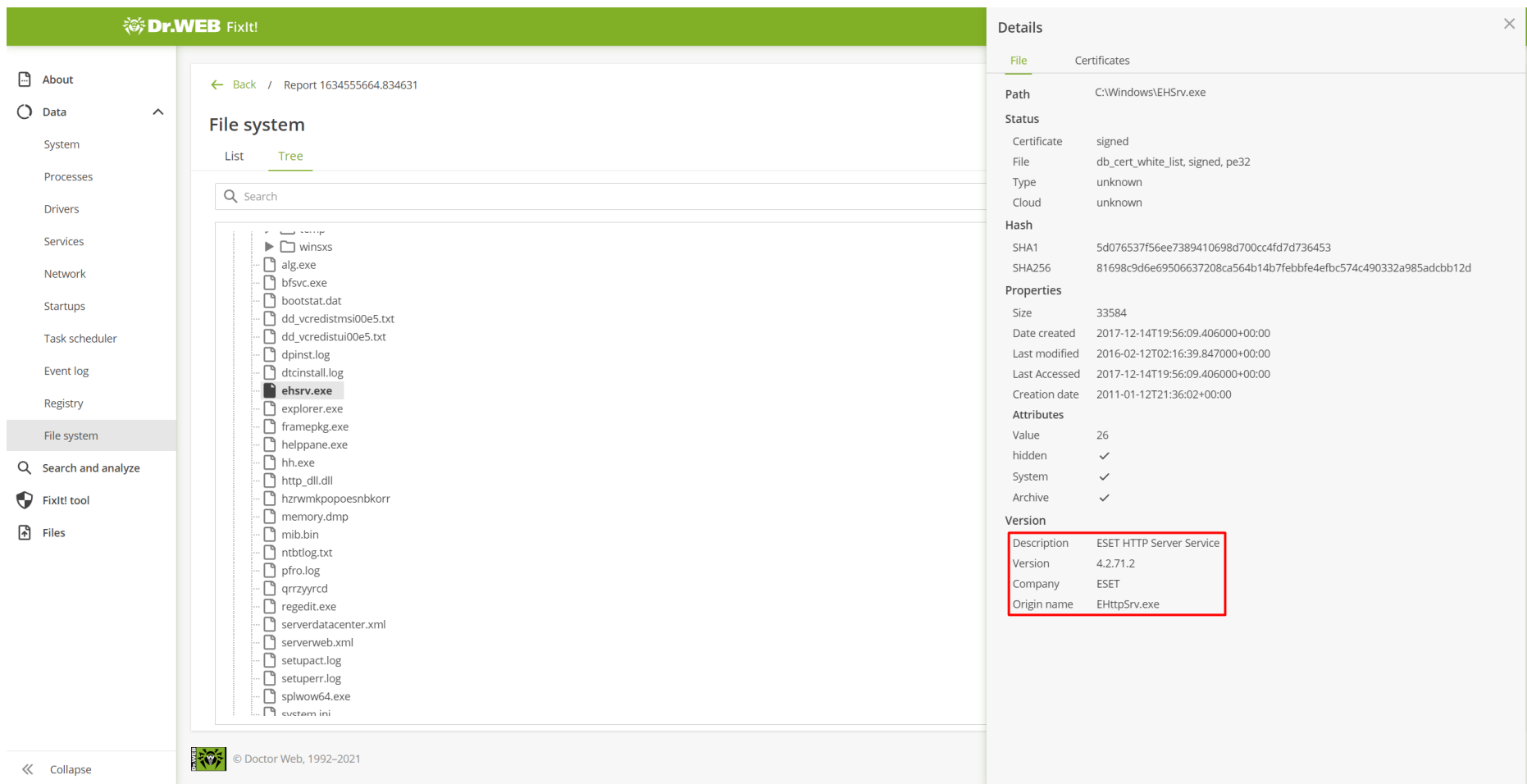


The screenshot shows the Dr.Web FixIt! application interface. On the left is a sidebar with navigation options: About, Data, System, Processes, Drivers, Services, Network, Startups, Task scheduler, Event log, Registry, File system (selected), Search and analyze, FixIt! tool, and Files. The main area displays a file system tree for a specific report (1634555664.834631). The tree shows various files and folders, with 'pdf.exe' highlighted. On the right, a 'Details' panel provides information about the selected file. The 'File' tab is active, showing the path 'C:\Windows\TEMP\pdf.exe', status, certificate, file name, type, cloud status, hash (SHA1 and SHA256), properties (size, date created, last modified, last accessed, creation date), attributes (value, archive), and version information. The version information is highlighted with a red box.

Details	
File Certificates	
Path	C:\Windows\TEMP\pdf.exe
Status	
Certificate	signed_microsoft
File	signed_microsoft, system_file_dualuse, pe32, sysinternals_tool
Type	sysint_procdump
Cloud	unknown
Hash	
SHA1	542e79418f5cfee03323b1aaff9b83423a20e310
SHA256	010e32be0f86545e116a8bc3381a8428933eb8789f32c261c81fd5e7857d4a77
Properties	
Size	543928
Date created	2019-01-16T01:57:02.011000+00:00
Last modified	2015-04-17T12:54:19+00:00
Last Accessed	2019-01-16T01:57:02.011000+00:00
Creation date	2014-07-04T03:34:09+00:00
Attributes	
Value	20
Archive	✓
Version	
Description	Sysinternals process dump utility
Version	7.01
Company	Sysinternals - www.sysinternals.com
Origin name	procdump



Ищем APT backdoor



The screenshot displays the Dr.Web FixIt! application interface. On the left is a navigation sidebar with categories like About, Data, System, Processes, Drivers, Services, Network, Startups, Task scheduler, Event log, Registry, File system, Search and analyze, FixIt! tool, and Files. The 'File system' category is selected. The main area shows a file tree for 'Report 1634555664.834631'. The file 'ehsrv.exe' is highlighted. On the right, a 'Details' panel provides information about the selected file.

File system

Back / Report 1634555664.834631

List Tree

Search

ehsrv.exe

Details

File Certificates

Path C:\Windows\EHsrv.exe

Status

Certificate signed

File db_cert_white_list, signed, pe32

Type unknown

Cloud unknown

Hash

SHA1 5d076537f56ee7389410698d700cc4fd7d736453

SHA256 81698c9d6e69506637208ca564b14b7febbfe4efbc574c490332a985adccb12d

Properties

Size 33584

Date created 2017-12-14T19:56:09.406000+00:00

Last modified 2016-02-12T02:16:39.847000+00:00

Last Accessed 2017-12-14T19:56:09.406000+00:00

Creation date 2011-01-12T21:36:02+00:00

Attributes

Value 26

hidden ✓

System ✓

Archive ✓

Version

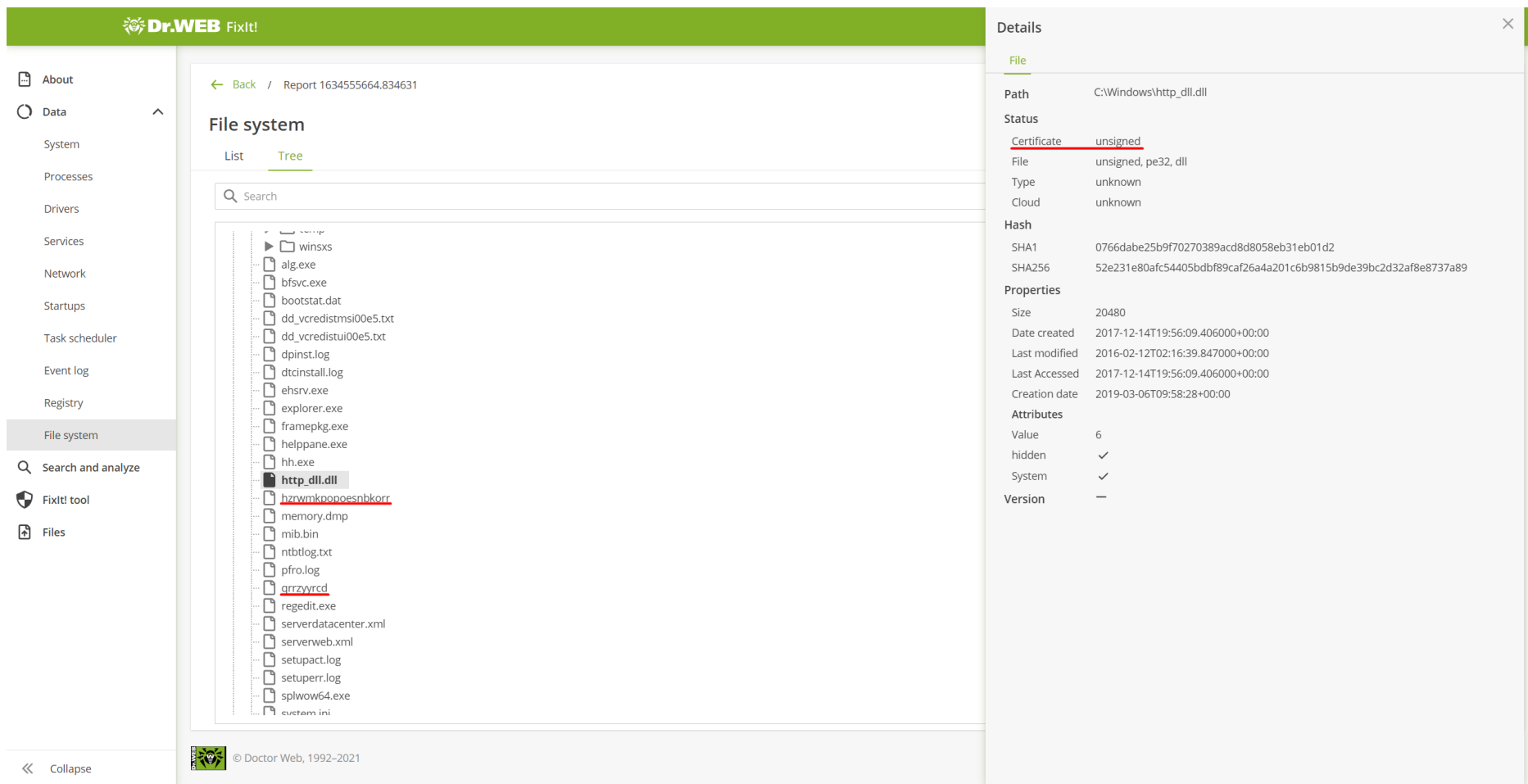
Description ESET HTTP Server Service

Version 4.2.71.2

Company ESET

Origin name EHttrv.exe

Ищем APT backdoor



The screenshot displays the Dr.Web FixIt! application interface. The left sidebar contains navigation options: About, Data, System, Processes, Drivers, Services, Network, Startups, Task scheduler, Event log, Registry, File system (selected), Search and analyze, FixIt! tool, and Files. The main window shows a file system tree for Report 1634555664.834631. The file **http.dll** is highlighted, and its details are shown on the right. The details pane includes sections for File, Status, Hash, Properties, and Attributes.

File	
Path	C:\Windows\http.dll
Status	
Certificate	unsigned
File	unsigned, pe32, dll
Type	unknown
Cloud	unknown
Hash	
SHA1	0766dabe25b9f70270389acd8d8058eb31eb01d2
SHA256	52e231e80afc54405bdbf89caf26a4a201c6b9815b9de39bc2d32af8e8737a89
Properties	
Size	20480
Date created	2017-12-14T19:56:09.406000+00:00
Last modified	2016-02-12T02:16:39.847000+00:00
Last Accessed	2017-12-14T19:56:09.406000+00:00
Creation date	2019-03-06T09:58:28+00:00
Attributes	
Value	6
hidden	✓
System	✓
Version	—

Ищем APT backdoor

▼ Hacktools software								
Action ▼	Type ↕	Path ↕	hash.sha256 ↕	arkstatus.file ↕	arkstatus.cert ↕	certinfo.item.subje...	verinfo.version ↕	verinfo.company ↕
☐ None ▼	Files	C:\Windows\TEMP\pdf.exe	> 010e32be0f86545...	▼ [signed_microsoft,system_file_dualuse,pe32,sysinternals_tool]	> [signed_microsoft]	> Microsoft Corpora...	7.01	▼ Sysinternals - www.sysinternals.com



Ищем APT backdoor

▼ Unsigned untrusted executables

Action ▾	Type ▾	Path ▾	hash.sha256 ▾	arkstatus.file ▾	verinfo.version ▾	verinfo.company ▾
☐ None ▼	Files	<u>C:\Windows\http.dll</u>	➤ 52e231e80afc54405bdbf89...	➤ [unsigned,pe32,dll]	—	—
☐ None ▼	Files	<u>C:\Windows\IME\RasTls.dll</u>	➤ 58ea31a5a8711a99ae26b6...	➤ [unsigned,pe32,dll]	—	—
☐ None ▼	Files	C:\Windows\SysWOW64\mfc71.dll	➤ 4da5efdc46d126b45daeee8...	➤ [unsigned,pe32,dll]	7.10.3077.0	Microsoft Corporation
☐ None ▼	Files	C:\ProgramData\MISICS\MISICS.dll	➤ f0b967ca98f9b0b9009cf741...	➤ [unsigned,pe64,dll]	10.0.10240.16390	Microsoft Corporation
☐ None ▼	Files	C:\Windows\SysWOW64\mfc71u.dll	➤ 0c58f682e1b3af064963dd6...	➤ [unsigned,pe32,dll]	7.10.3077.0	Microsoft Corporation
☐ None ▼	Files	C:\Windows\FramePkg.exe	➤ ae7b31534349537f59cb8a1...	➤ [unsigned,pe32]	4.8.0.641	McAfee, Inc.
☐ None ▼	Files	C:\ProgramData\AppData\msvsct.exe	➤ cbbffe0d67d2aa49df1e069c...	➤ [unsigned,pe32]	—	—
☐ None ▼	Files	C:\Windows\SysWOW64\msvcr71.dll	➤ 8094af5ee310714caebccae...	➤ [unsigned,pe32,dll]	7.10.3052.4	Microsoft Corporation
☐ None ▼	Files	<u>C:\Windows\TEMP\RasTls.dll</u>	➤ efae0109e730c6b8a50dfbe...	➤ [unsigned,pe32,dll]	—	—
☐ None ▼	Files	<u>C:\Windows\System32\oci.dll</u>	➤ e7b50c499cd9ec8efa9150a...	➤ [unsigned,pe64,dll]	11.2.0.1	—
☐ None ▼	Files	C:\Program Files\VMware\VMware Tools\sigc-2.0.dll	➤ 0a5cd7ada051466ef7100c0...	➤ [unsigned,pe64,dll]	2.2.9	➤ The libsigc++ development t...



Кейс №2

Майнер

- **Обращение от пользователя:**

Добрый день! У меня проблема. Скорее всего я поймал вирус-майнер.

Сначала ПК как будто подзавис, я думал подожду, оклемается.

Свернув окно рабочей программы я обнаружил, что найден и обезврежен вирус. Я перезагрузился и по всем признакам это майнер (грузит ЦП и оперативку).

Пожалуйста помогите.



Майнер

▼ Metawave detects

Action ⚡	Type ⚡	Path ▲	hash.sha1 ⚡	analysis_results.metawave.result ⚡
☐ None ▼	Files	<u>C:\ProgramData\Windows\dlchosts.exe</u>	5bc9cc1abde7553966663ac910ceb66fb98cef32	infected
☐ None ▼	Files	<u>C:\programdata\windows\xmrig-cuda.dll</u>	ad1f9eb487326af9a7f983969d7042935ebd48ff	infected
☐ None ▼	Files	➤ C:\Program Files\GRAPHISOFT\ArchiCAD 16\Расшир...	f6a1765f8fb633885099823b55da0a0012a85ebf	suspicious_vendor
☐ None ▼	Files	➤ C:\Program Files (x86)\ArtMoney Pro 7.44.1 Portable ...	7e955ca900100f31c80d21f6d66e28851e7c6ea4	suspicious_vendor
☐ None ▼	Files	C:\Program Files (x86)\uTorrent\utorrent.exe	8ac172017f92c0ca70f200cdda017fc96764b8dd	suspicious_vendor
☐ None ▼	Files	➤ C:\Users\Администратор\AppData\Roaming\uTorre...	6cdb63909ce09c1e2aaab14a7b174df87060d4cf	suspicious_vendor
☐ None ▼	Files	C:\Windows\system32\dbgeng.dll	55e633666cd73ac1fad12c6a78ed8256fbe84593	suspicious
☐ None ▼	Files	C:\Windows\System32\dbghelp.dll	8835dbda73b15f87cceedfe707b9166bad409440	suspicious
☐ None ▼	Files	C:\Windows\SysWOW64\dbgeng.dll	95b28a077bc256eda1692ed4c5f1e8d75d1cbc3b	suspicious
Action ▼	Type ⚡	Path ⚡	Threat ⚡	Type ⚡
☐ None ▼	Signature det...	<u>C:\programdata\windows\xmrig-cuda.dll</u>	<u>Tool.BtcMine.2405</u>	hacktool



Майнер

▼ Suspicious software

Action ↕	Type ↕	Path ↕	hash.sha256 ↕	arkstatus.file ↕	arkstatus.cert ↕	certinfo.item.subject.cn ↕	verinfo.version ↕	verinfo.company ↕
☐ None ▼	Files	▼ C:\programdata\windows\WinRing0x64.sys	➤ 11bd2c9f9e2397...	➤ [ts_white_list,db_...	[signed]	➤ Noriyuki MIYAZAKI,GlobalSig...	1.2.0.5	OpenLibSys.org



Майнер

Поиск и анализ

 Готовые фильтры  **Новый фильтр**  Выбранные действия

+ Мои фильтры

dlchosts

Path,hash.sha1,arkstatus.file,key,display_name

Применить

Сохранить как новый фильтр

Действие ↕	Тип ↕	Путь ▲	hash.sha1 ↕	arkstatus.file ↕	Ключ ↕	display_name ↕
☐ None ▼	Запланированные задания	C:\programdata\windows\dlchosts.exe	—	—	—	—
☐ —	Сетевые подключения	C:\ProgramData\Windows\dlchosts.exe	—	—	—	—
☐ None ▼	Процессы	C:\ProgramData\Windows\dlchosts.exe	—	—	—	—
☐ None ▼	Файлы	C:\ProgramData\Windows\dlchosts.exe	> 5bc9cc1abde755396663ac9...	[unsigned,pe64,new_pe]	—	—



Майнер

Поиск и анализ

 Готовые фильтры  Новый фильтр  **Выбранные действия (4)**

 Создать  Обновить

▼ Запланированные задания

Действие ↕	Тип ↕	Имя ↕	Команда ↕
Delete ▼	mstasks	\Microsoft\Windows\Maintenance\WinDAT	C:\ProgramData\Windows\cmd /c dlhosts.exe dlchosts.exe

▼ Файлы

Действие ↕	Тип ↕	Путь ↕	SHA1 ↕	signed ↕
Disinfect ▼	Файлы	C:\programdata\windows\WinRing0x64.sys	—	—
Disinfect ▼	Файлы	C:\ProgramData\Windows\dlchosts.exe	—	—
Disinfect ▼	Файлы	C:\programdata\windows\xmrig-cuda.dll	—	—



Кейс #3

Бесфайловая PowerShell угроза

- Предыстория
 - Обращение от пользователя: подозрение на майнер на сервере.
 - Исследуется сервер с подозрением на заражение.



Бесфайловая PowerShell угроза

▼ WMI PowerShell Malware					
Действие ▼	Тип ↕	Экземпляр ↕	Данные ↕	Угроза ↕	
☐ None ▼	WMI	> \\VIRT2\ROOT\subscription:CommandLineEventConsu...	> powershell -NoP -NonI -W Hidden -exec bypass -E DQA...	—	
☐ None ▼	WMI	> \\VIRT2\ROOT\subscription:CommandLineEventConsu...	> powershell -NoP -NonI -W Hidden -exec bypass -E DQA...	WMI:SUSPICIOUS.Data	

▼ XMRig				
Действие ▼	Тип ↕	Путь ↕	hash.sha256 ↕	arkstatus.file ↕
☐ None ▼	Файлы	C:\Windows\TEMP\6982734\setup_49182.exe	> c115b7f348cdd670c81ec16035e6ce0307e78784d9421c...	[unsigned,pe64]

▼ Metawave detects				
Действие ▼	Тип ↕	Путь ↕	hash.sha1 ↕	analysis_results.metawave.result ↕
☐ Disinfect ▼	Файлы	C:\Windows\TEMP\6982734\setup_49182.exe	c3680105fcd1169e09406fb7983842eaf110d936	suspicious_vendor

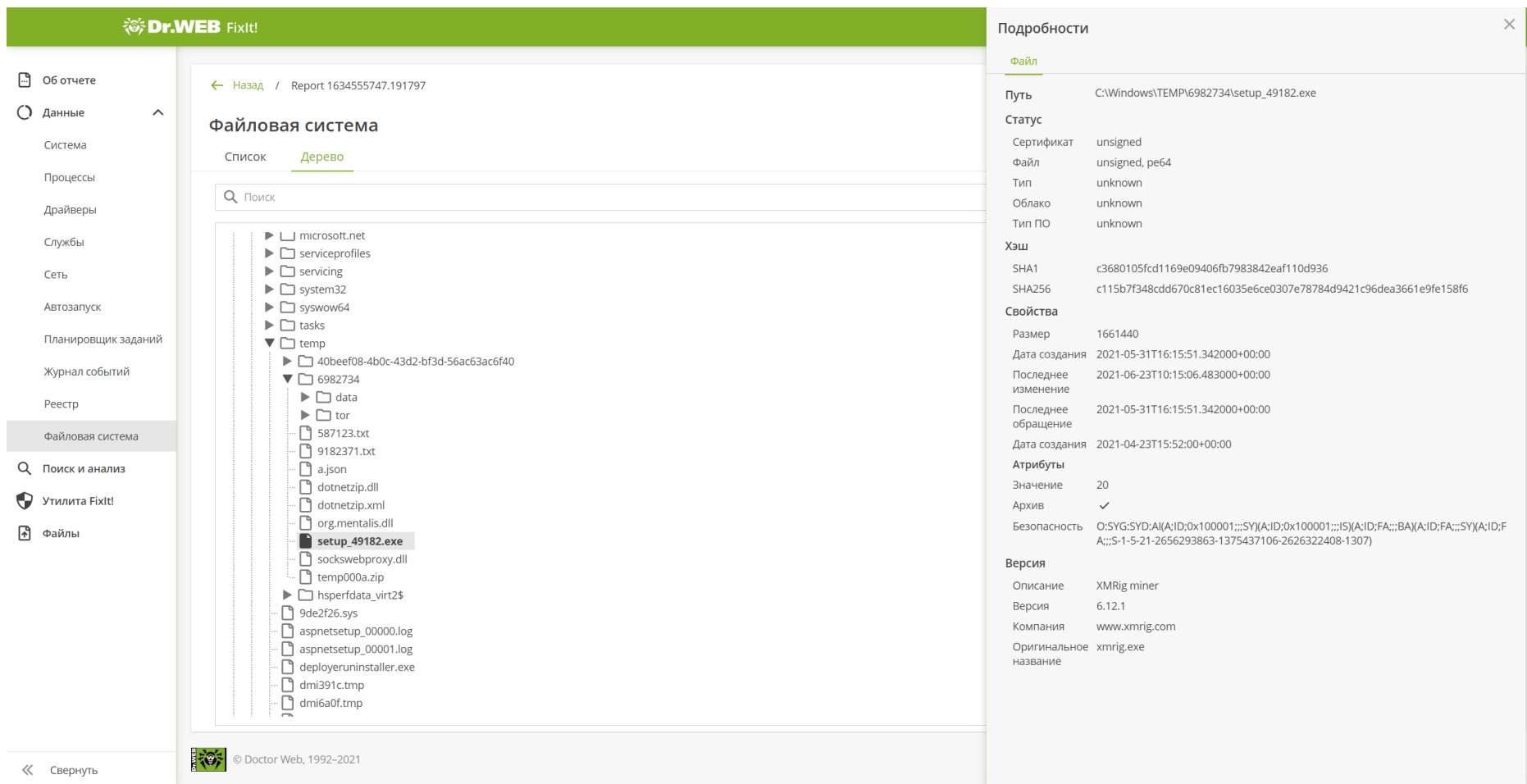


Бесфайловая PowerShell угроза

☐	None ▼	Файлы	C:\Windows\TEMP\6982734\DotNetZip.dll	> 698e4beeba26363e632cbbb...	> [unsigned,pe32,dll,dot_net]	1.15.0
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Org.Mentalis.dll	> 9569755c419e5de9b48d430c...	> [unsigned,pe32,dll,dot_net]	1.0.0.0
☐	Disinfect ▼	Файлы	C:\Windows\TEMP\6982734\setup_49182.exe	> c115b7f348cdd670c81ec160...	[unsigned,pe64]	6.12.1
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\SocksWebProxy.dll	> 8c2657fc9588f2b5bdf609af9...	> [unsigned,pe32,dll,dot_net]	1.0.5.0
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\libcrypto-1_1.dll	> 6b030d7357e8f3f2d14c03fba...	[unsigned,pe32,dll]	1.1.1k
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\libevent-2-1-7.dll	> 9fc30ffc9b3f5661a026a2d54...	[unsigned,pe32,dll]	—
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\libevent_core-2-1-7.dll	> 0d5583a23da843bf10397cad...	[unsigned,pe32,dll]	—
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\libevent_extra-2-1-7.dll	> 9aa9ea2181c3b95f44cd6707...	[unsigned,pe32,dll]	—
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\libgcc_s_sjlj-1.dll	> 30a46397aef0d6132924a3af...	[unsigned,pe32,dll]	—
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\libssl-1_1.dll	> d34003f0521d375c21f24200...	[unsigned,pe32,dll]	1.1.1k
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\libssp-0.dll	> 0650d1e0ceafe784aa4bc161...	[unsigned,pe32,dll]	—
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\libwinpthread-1.dll	> cdce5532df5a087afe8034cc0...	[unsigned,pe32,dll]	1, 0, 0, 0
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\setup000.exe	> 5e300b3112dd2792c0da2ccc...	[unsigned,pe32]	—
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\tor.exe	> 5e300b3112dd2792c0da2ccc...	[unsigned,pe32]	—
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\tor-gencert.exe	> ecec6461412827fcf817e6044...	[unsigned,pe32]	—
☐	None ▼	Файлы	C:\Windows\TEMP\6982734\Tor\zlib1.dll	> a8c08a07a463475eec8b87b4...	[unsigned,pe32,dll]	1.2.11
☐	None ▼	Файлы	C:\Windows\TEMP\DeployerUnInstaller.exe	> 798b9f5c29a09d525c20bd01...	[unsigned,pe32]	9.0.0.902
☐	None ▼	Файлы	C:\Windows\TEMP\setup_00.exe	> f28135ce43302683d518fd67...	[unsigned,pe32]	—



Бесфайловая PowerShell угроза



Dr.WEB FixIt!

Об отчете
Данные
Система
Процессы
Драйверы
Службы
Сеть
Автозапуск
Планировщик заданий
Журнал событий
Реестр
Файловая система
Поиск и анализ
Утилита FixIt!
Файлы

Назад / Report 1634555747.191797

Файловая система

Список Дерево

Поиск

- microsoft.net
- serviceprofiles
- servicing
- system32
- syswow64
- tasks
- temp
 - 40beef08-4b0c-43d2-bf3d-56ac63ac6f40
 - 6982734
 - data
 - tor
 - 587123.txt
 - 9182371.txt
 - a.json
 - dotnetzip.dll
 - dotnetzip.xml
 - org.mentalis.dll
 - setup_49182.exe**
 - sockswebproxy.dll
 - temp000a.zip
 - hspferdata_virt2\$
 - 9de2f26.sys
 - aspnetsetup_00000.log
 - aspnetsetup_00001.log
 - deployeruninstaller.exe
 - dmi391c.tmp
 - dmi6a0f.tmp

Свернуть

© Doctor Web, 1992–2021

Подобности

Файл

Путь: C:\Windows\TEMP\6982734\setup_49182.exe

Статус

Сертификат	unsigned
Файл	unsigned, pe64
Тип	unknown
Облако	unknown
Тип ПО	unknown

Хэш

SHA1	c3680105fcd1169e09406fb7983842eaf110d936
SHA256	c115b7f348cdd670c81ec16035e6ce0307e78784d9421c96dea3661e9fe158f6

Свойства

Размер	1661440
Дата создания	2021-05-31T16:15:51.342000+00:00
Последнее изменение	2021-06-23T10:15:06.483000+00:00
Последнее обращение	2021-05-31T16:15:51.342000+00:00
Дата создания	2021-04-23T15:52:00+00:00

Атрибуты

Значение	20
Архив	✓
Безопасность	O:SYG:SYD:AI(A;ID;0x100001;;;SY)(A;ID;0x100001;;;IS)(A;ID;FA;;;BA)(A;ID;FA;;;SY)(A;ID;FA;;;S-1-5-21-2656293863-1375437106-2626322408-1307)

Версия

Описание	XMRig miner
Версия	6.12.1
Компания	www.xmrig.com
Оригинальное название	xmrig.exe



Вопросы?

- Демо-версия: <https://download.drweb.com/fixit/>



У вас есть что защитить? У нас есть Dr.Web



Напишите

<https://antivirus.pf/>
поддержка



Позвоните

8 800 33 79 32



Закажите звонок

через форму на сайте

