

# RSA<sup>®</sup>Conference2020 Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

**HUMAN**  
ELEMENT

SESSION ID: EFT-R08

## It Hurt Itself in Confusion: No distribute scanners and stealthy malware

**Mathieu Gaucheler**

Cybersecurity Analyst  
Blueliv  
@shibasec

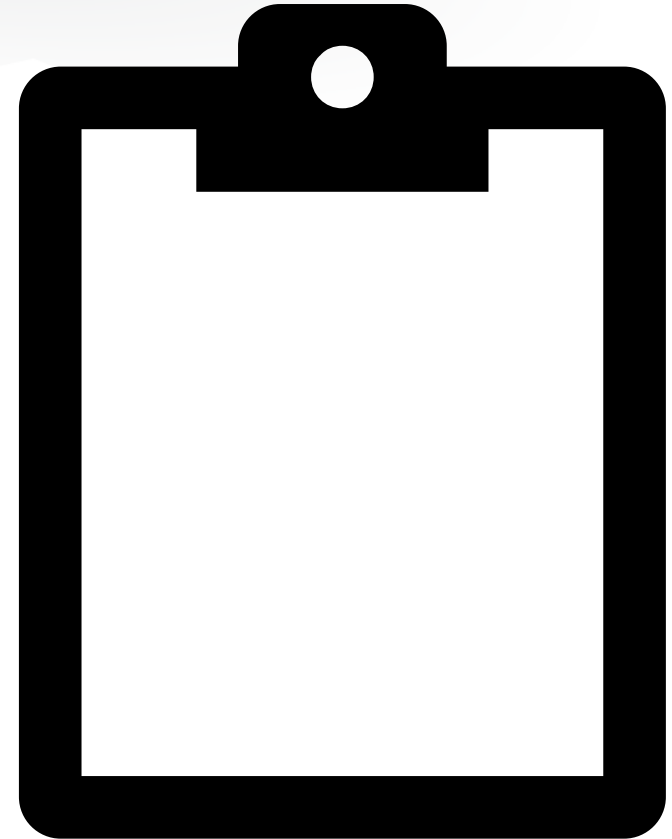
**Liv Rowley**

Threat Intelligence Analyst  
Blueliv  
@OLRowley



# Agenda

- No Distribute Scanners 101
- Overview of Different NDS Services
- NDS in the Cybercriminal Landscape
- Key Points



**RSA**®Conference2020 **APJ**

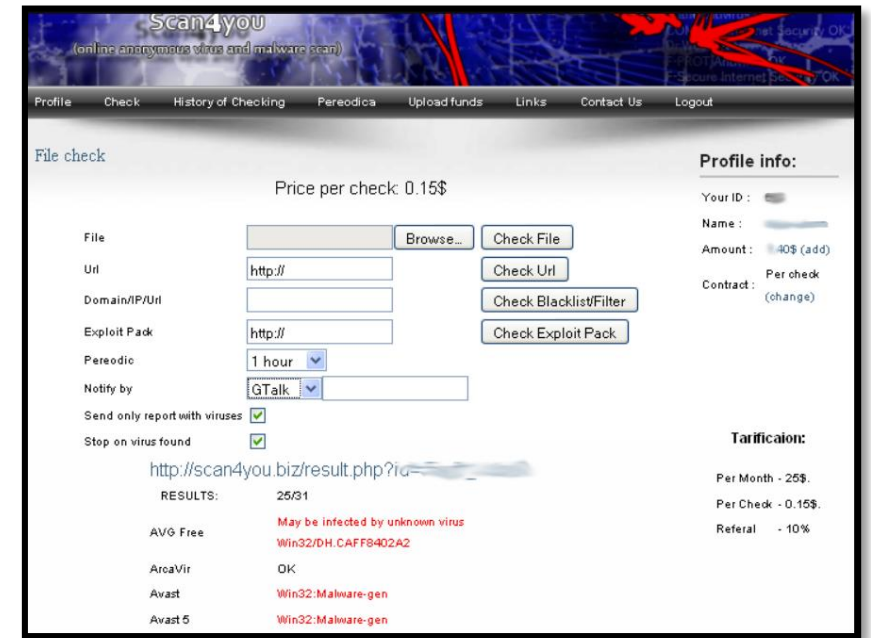
---

A Virtual Learning Experience

## Case Study: Scan4You & Dyncheck

# Scan4You

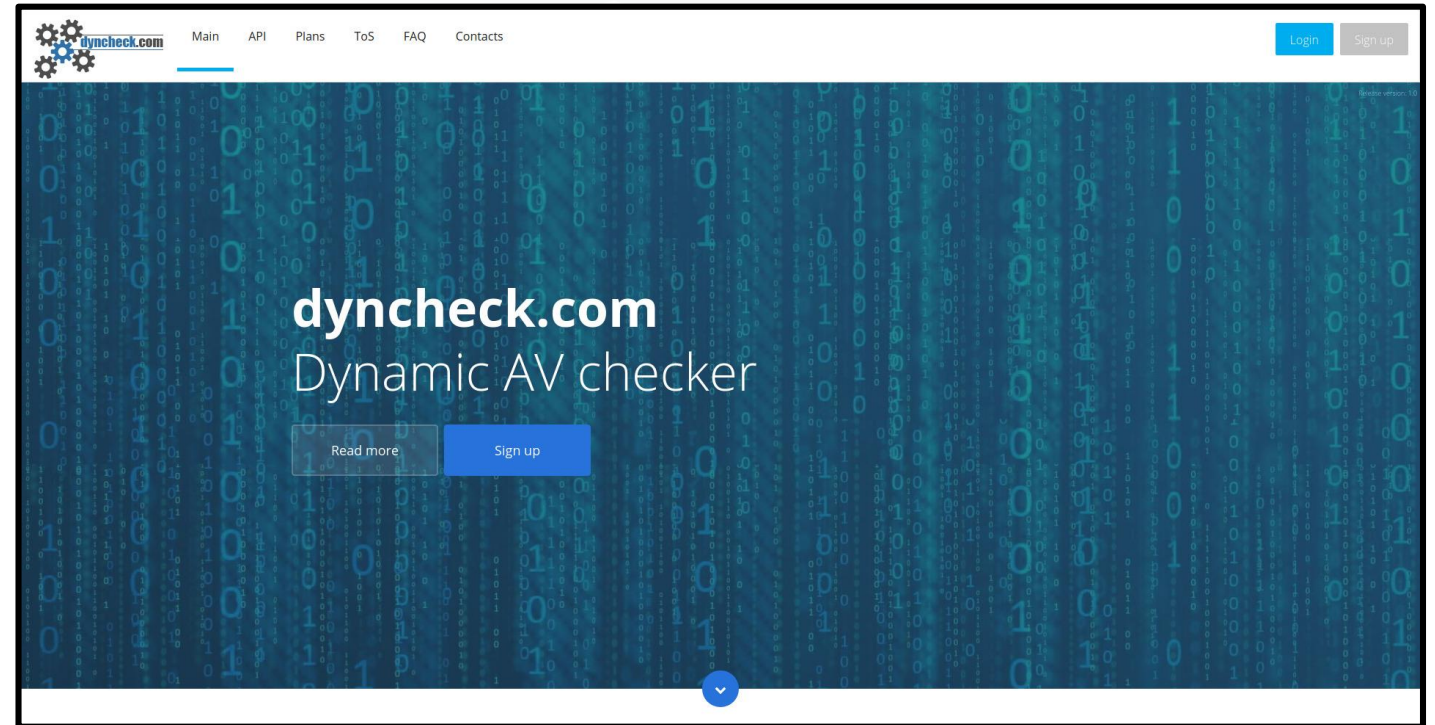
- "VirusTotal-for-Crooks"
- 2009-2017
- 30,000 registered users
- 14 year prison sentence



*Credit: Krebs on Security*

# DynCheck

- Top no distribute scanner (NDS) in 2020
- Appeared in 2016
- Static & dynamic scans



**RSA**<sup>®</sup>Conference2020 **APJ**

---

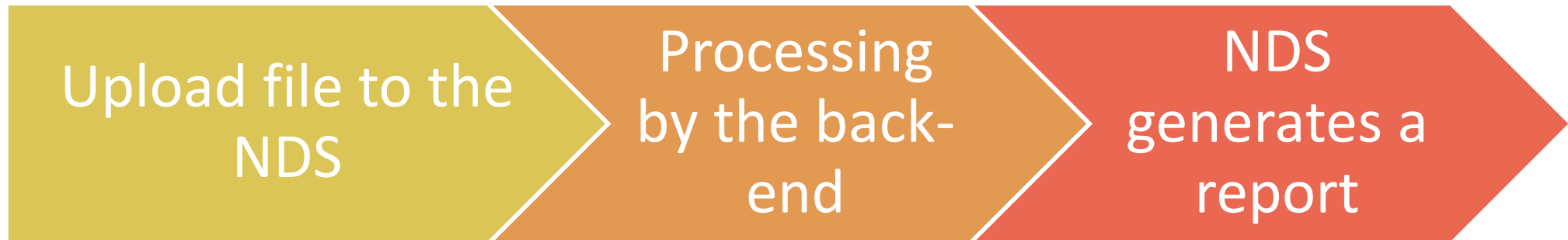
A Virtual Learning Experience

# No Distribute Scanners 101



# What are NDSs?

- Standalone websites
- Scan files against dozens of antivirus products
- No feedback loop
- Marketed to cybercriminals





Free scan: Available

Drop file here  
or  
Click to upload

Please enter your token here or leave blank for f

500 x 75

BEST CRYPTER



500 x 75



Select your method of deployment

Load File



Click here to select a file or drag it into the field below.









































## Parameters

Export function



- ☐ Enable Internet  
(your file may be distributed)
- ☐ Delete Zone.Identifier  
(before file execution)
- ☐ Enable macros content  
(autorun macro-enabled doc\* files)
- ☐ Disable UAC  
(unrestricted system access)
- ☐ Use DbgView  
(during file execution)
- ☐ Move Mouse  
(before file execution)
- ☐ Scantime    ☐ Runtime

## Select which antiviruses to include in the scan

- |   |   |
|---|---|
| <input type="checkbox"/>  360 Total Security | <input type="checkbox"/>  Nano AV            |
| <input type="checkbox"/>  Adaware            | <input type="checkbox"/>  Norton             |
| <input type="checkbox"/>  Arcabit            | <input type="checkbox"/>  Panda              |
| <input type="checkbox"/>  Avast              | <input type="checkbox"/>  Quickheal          |
| <input type="checkbox"/>  AVG                | <input type="checkbox"/>  Rising             |
| <input type="checkbox"/>  Avira              | <input type="checkbox"/>  Sophos             |
| <input type="checkbox"/>  Bitdefender        | <input type="checkbox"/>  Super Anti-Spyware |
| <input type="checkbox"/>  Bullguard          | <input type="checkbox"/>  Symantec           |
| <input type="checkbox"/>  Cylance            | <input type="checkbox"/>  Total AV           |
| <input type="checkbox"/>  Comodo             | <input type="checkbox"/>  Total Defense      |
| <input type="checkbox"/>  Dr Web             | <input type="checkbox"/>  Trustport          |
| <input type="checkbox"/>  Emsisoft           | <input type="checkbox"/>  Trend Micro        |
| <input type="checkbox"/>  EScan              | <input type="checkbox"/>  VIPRE              |
| <input type="checkbox"/>  ESET NOD32         | <input type="checkbox"/>  VBA32              |
| <input type="checkbox"/>  F-Protect          | <input type="checkbox"/>  Webroot            |
| <input type="checkbox"/>  F-Secure         | <input type="checkbox"/>  Windows Defender |
| <input type="checkbox"/>  GData            | <input type="checkbox"/>  Zillya           |
| <input type="checkbox"/>  K7 Computing     | <input type="checkbox"/>  ZoneAlarm        |
| <input type="checkbox"/>  Kaspersky        |   |
| <input type="checkbox"/>  Malwarebytes     |   |
| <input type="checkbox"/>  MAX Secure       |   |
| <input type="checkbox"/>  McAfee           |   |

☐ Select all

Antivirus information

SCAN FILE



**RSA**®Conference2020 **APJ**

---

A Virtual Learning Experience

## Overview of Different NDS Services

# Antivirus 101: static VS dynamic

- Static analysis
  - String detection
  - Format analysis
  - Entropy analysis
- Dynamic analysis
  - Monitoring
  - Process memory analysis
  - Emulation

```

298 rule XProtect_OSX_HiddenLotus_A
299 {
300     meta:
301         description = "OSX.HiddenLotus.A"
302     strings:
303         $a1 = { 00 2F 00 25 6C 64 00 00 00 00 00 00 00 00 00 00 }
304         $a2 = { 00 72 62 00 00 20 26 00 00 00 00 00 00 00 }
305         $a3 = { 00 25 64 00 20 32 3E 26 31 00 72 00 0D 0A 00 00 }
306         $a4 = { 00 25 30 32 78 00 00 00 00 00 00 00 }
307         $a5 = { 00 3D 00 3B 00 00 00 }
308     condition:
309         Macho and all of ($a*) and filesize < 180000
310 }
311
312 rule XProtect_OSX_Mughthesec_B
313 {
314     meta:
315         description = "OSX.Mughthesec.B"
316     strings:
317         $a1 = { 42 75 6E 64 6C 65 4D 65 55 70 }
318         $a2 = { 50 75 62 6C 69 73 68 65 72 4F 66 66 65 72 53 74 61 74 65 }
319         $a3 = { 49 6E 73 74 61 6C 6C 50 72 6F 67 72 65 73 73 53 74 61 74 65 }
320         $a4 = { 41 64 76 65 72 74 69 73 65 72 4F 66 66 65 72 53 74 61 74 65 }
321         $b1 = { 42 65 72 54 61 67 67 65 64 44 61 74 61 }
322         $b2 = { 42 45 52 50 72 69 6E 74 56 69 73 69 74 6F 72 }
323     condition:
324         Macho and filesize < 3000000 and all of them
325 }
326

```

# Static Scan

Runtime AV Check

Static AV Check

New scan task

Please browse the file or paste the link to start scan process...

Browse

Scan

Information

Static scan

Result

Detection rate: 1/31

AV	Detection
360 Total Security Essential	Clean
ALYac Internet Security	Clean
AVG Anti-Virus	Clean
Ad-Aware Antivirus	Clean
AhnLab V3 Light	Clean
Avast Antivirus	Clean
Avira Internet Security	Clean
BitDefender Total Security	Clean
BullGuard Internet Security	Clean
ClamAV	Clean
DrWeb Antivirus	Clean
Emsisoft Anti-Malware	Clean
Eset NOD32 Antivirus	Clean

DrWeb Antivirus	Clean
Emsisoft Anti-Malware	Clean
Eset NOD32 Antivirus	Clean
F-PROT Antivirus	Clean
F-Secure Anti-Virus	Clean
Fortinet Antivirus	Clean
G Data Internet Security	Clean
IKARUS anti.virus	Clean
K7 AntiVirus Premium	Clean
Kaspersky Internet Security	Clean
Malwarebytes Premium	Clean
McAfee Endpoint Protection	Clean
Norton Security	Heur.AdvML.B
Quick Heal Internet Security	Clean
Sophos Anti-Virus	Clean
TrustPort Antivirus Sphere	Clean
Vba32 AntiVirus Personal	Clean
Windows Defender	Clean
Zillya Antivirus	Clean
Zone Alarm Extreme Security	Clean
eScan Anti-Virus	Clean

Save as .pdf

Save as .jpg

Generate BBcodes

# Static Scan

Runtime AV Check	Static AV Check
New scan task	
Kaspersky Internet Security	Clean
Malwarebytes Premium	Clean
McAfee Endpoint Protection	Clean
Norton Security	Heur.AdvML.B
Quick Heal Internet Security	Clean
Sophos Anti-Virus	Clean
TrustPort Antivirus Sphere	Clean
BitDefender Total Security	Clean
BullGuard Internet Security	Clean
ClamAV	Clean
DrWeb Antivirus	Clean
Emsisoft Anti-Malware	Clean
Eset NOD32 Antivirus	Clean
Zillya Antivirus	Clean
Zone Alarm Extreme Security	Clean
eScan Anti-Virus	Clean

[Save as .pdf](#)
[Save as .jpg](#)
[Generate BBcodes](#)



# Dynamic Scan

Runtime AV Check

Static AV Check

New scan task

Please browse the file or paste the link to start scan process...

Browse

Scan

Information

Runtime scan

Result

Detection rate: 3/23

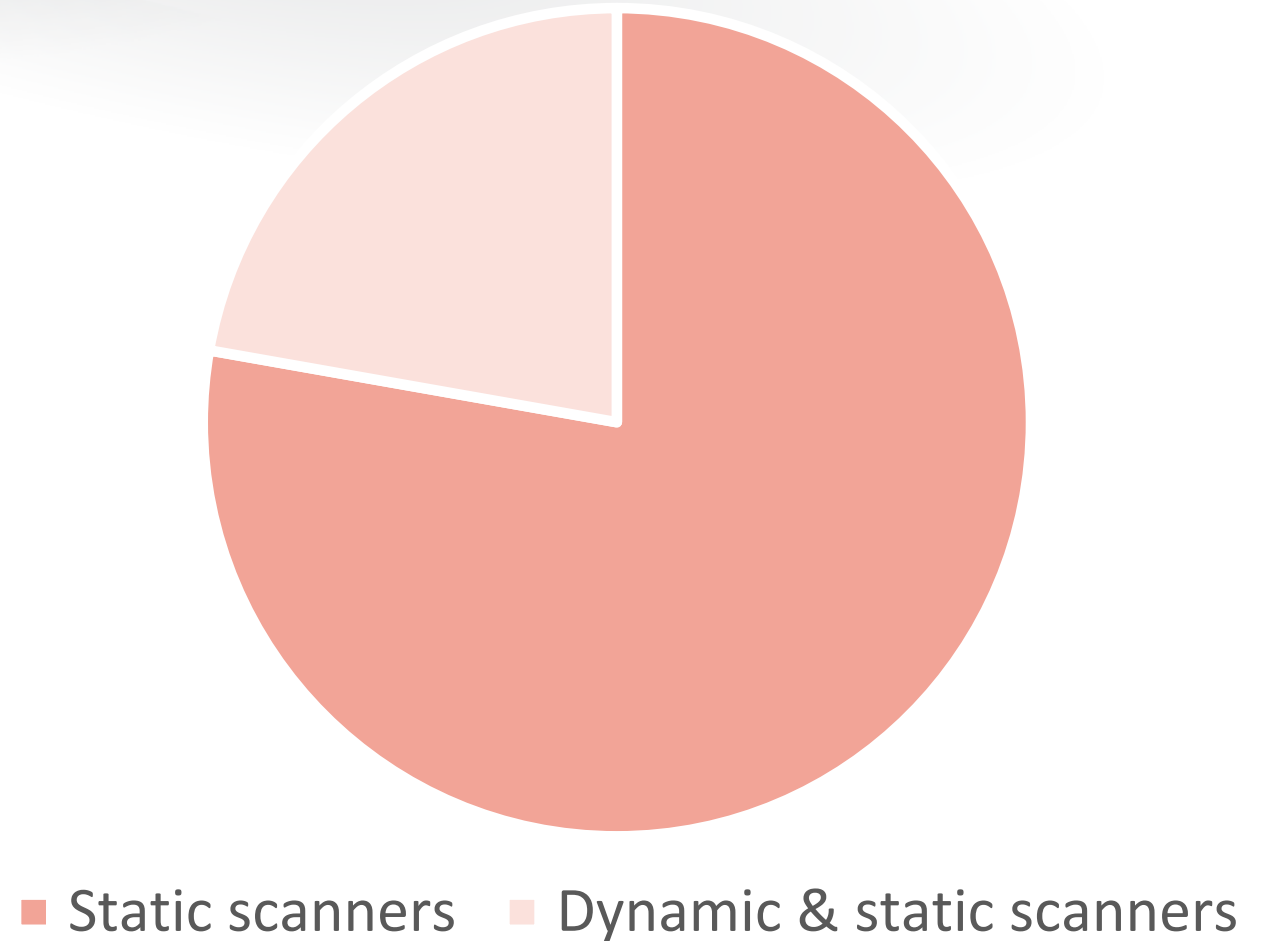
AV	Status	Alert Screen
360 Total Security Essential	Clean	
AVG Internet Security	Clean	
AhnLab V3 Light	Clean	
Avast Internet Security	Clean	
Avira Internet Security	Clean	
BitDefender Total Security	Clean	

DrWeb Total Security	Clean	
Emsisoft Anti-Malware	Clean	
Eset Smart Security	Clean	
F-Secure Internet Security	Clean	
Fortinet Smart Security	Clean	
Kaspersky Internet Security	Clean	
Malwarebytes Anti-Malware	Clean	
McAfee Internet Security	Clean	
Norton Internet Security	Dynamic detect after 5 sec.	
Panda Global Protection	Clean	
Sophos Anti-Virus	Clean	
Symantec Endpoint Security 14	Static detect	
Trend Micro Internet Security	Clean	
Webroot SecureAnywhere	Clean	
Windows Defender	Clean	

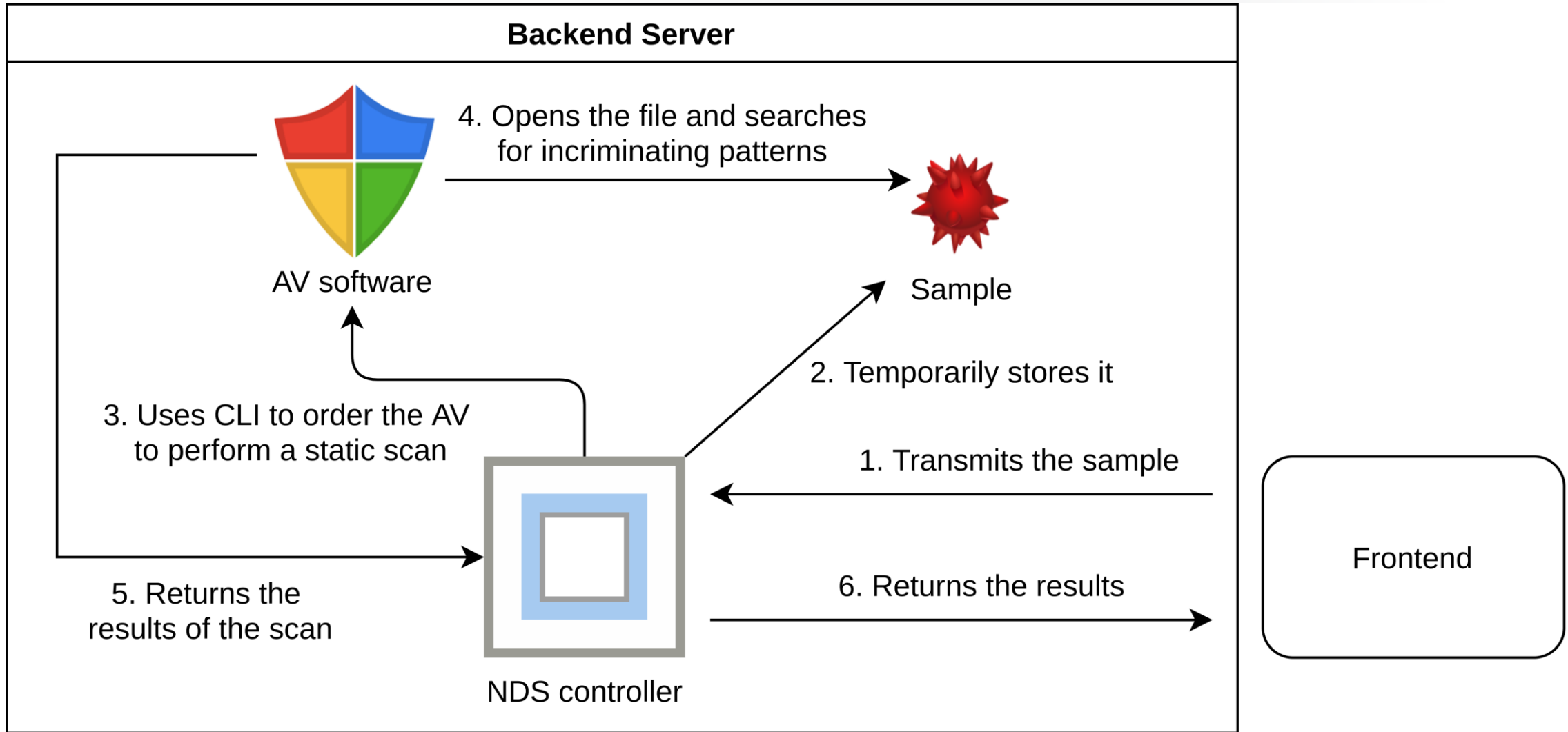


# Overview of NDS

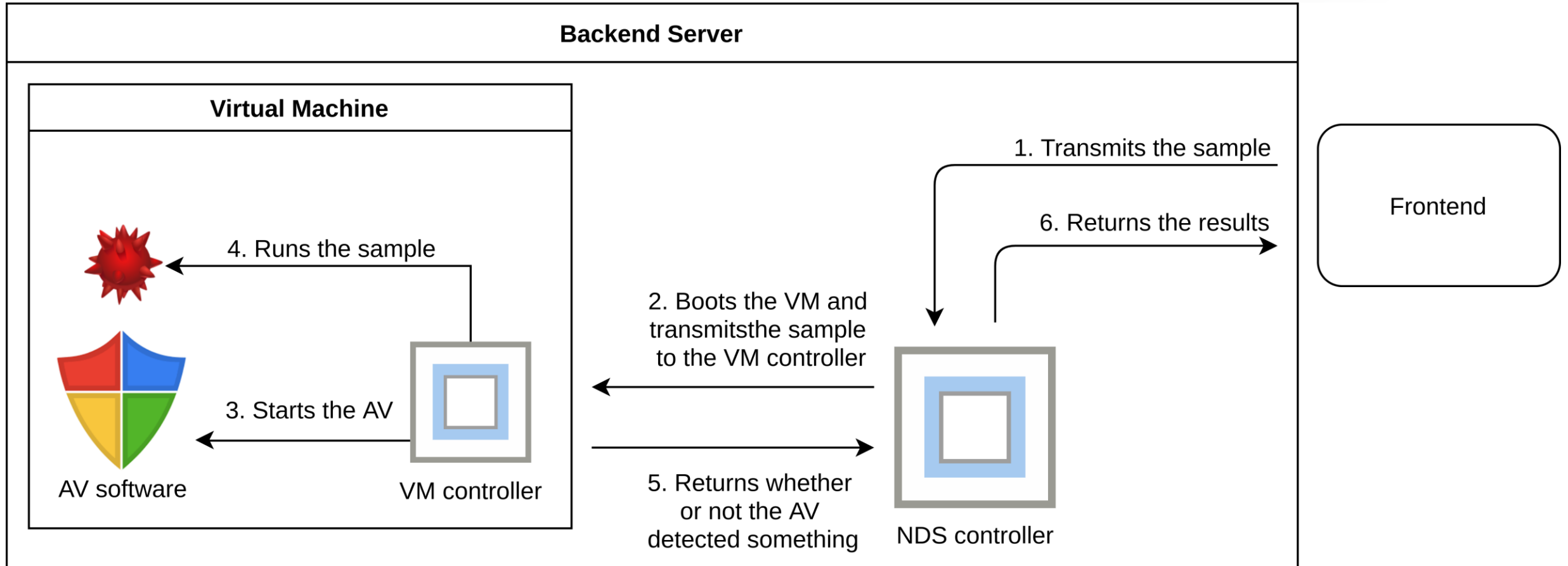
- Surveyed NDS: 9
- All offered API access
- Static scans offerings are much more common



# Possible static scanners architecture



# Possible dynamic scanner architecture



# What are the pricing models?



**Free models,**  
seemingly supported  
by paid advertising



**Single & bundle scan  
pricing** from \$0.01  
USD depending on  
provider



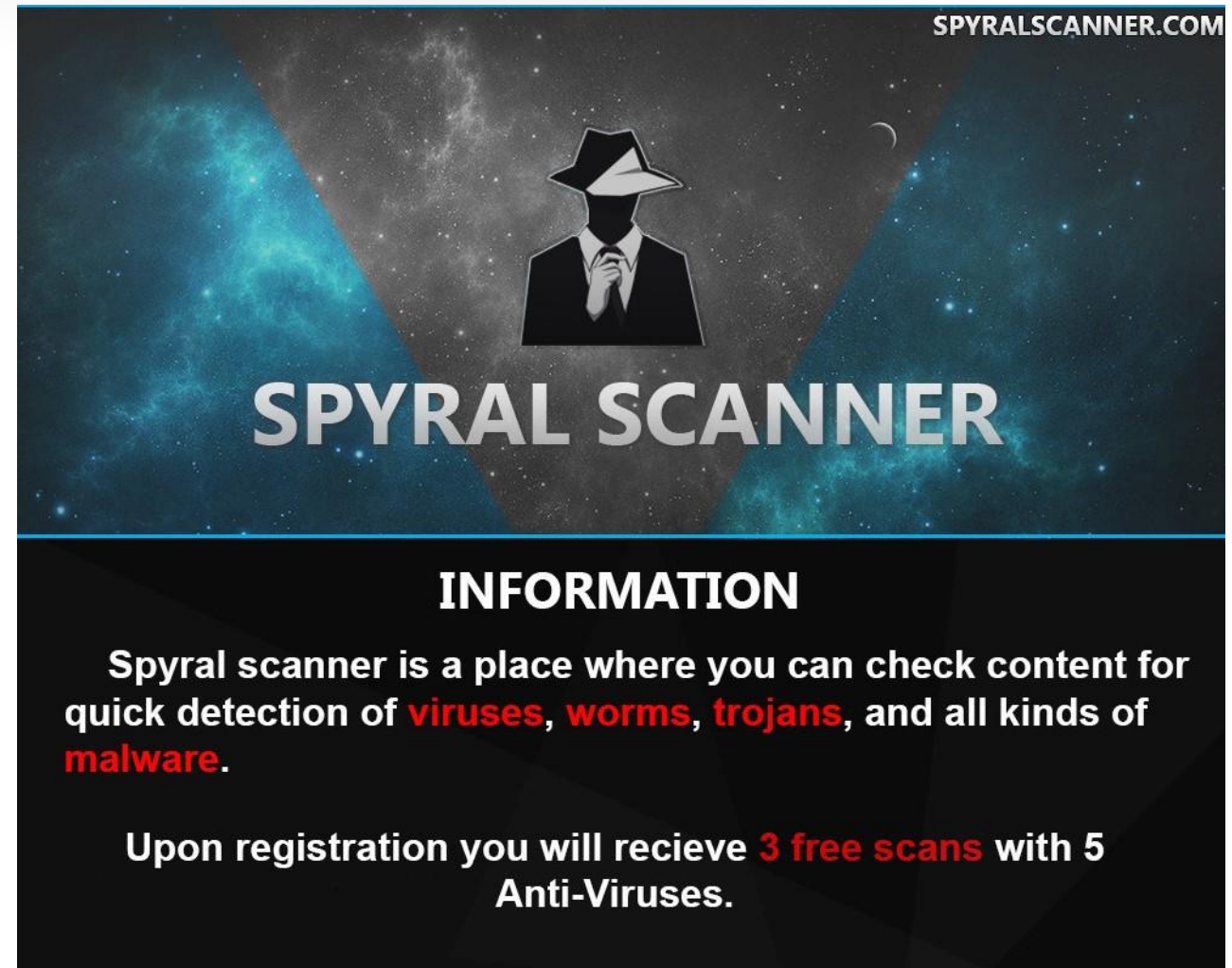
**Subscription-based  
models** range from  
\$50 to \$299 USD per  
month



# How are NDS services advertised?

*“At ScanHaven, you can scan your file on 39 fully licensed anti-viruses which include DAILY automated database updates”*

*- ScanHaven ad*

The advertisement for SPYRAL SCANNER features a dark, space-themed background with blue nebulae and a central figure in a black suit and white fedora. The text 'SPYRAL SCANNER' is prominently displayed in white. Below this, the word 'INFORMATION' is written in white. The main body of text describes the service as a place for quick detection of viruses, worms, trojans, and malware. It also mentions that upon registration, users will receive 3 free scans with 5 Anti-Viruses. The website 'SPYRALSCANNER.COM' is visible in the top right corner.

SPYRALSCANNER.COM

## SPYRAL SCANNER

### INFORMATION

Spyral scanner is a place where you can check content for quick detection of **viruses, worms, trojans**, and all kinds of **malware**.

Upon registration you will recieve **3 free scans** with 5 Anti-Viruses.

**RSA**®Conference2020 **APJ**

---

A Virtual Learning Experience

# The role of NDSs in the criminal landscape

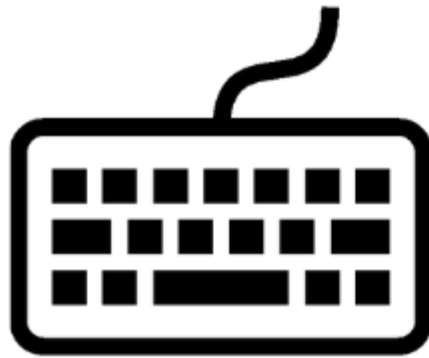
**RSA**®Conference2020 **APJ**

---

A Virtual Learning Experience

**NDS used directly by malware  
developers**

# When are NDS used in a malware life



Development

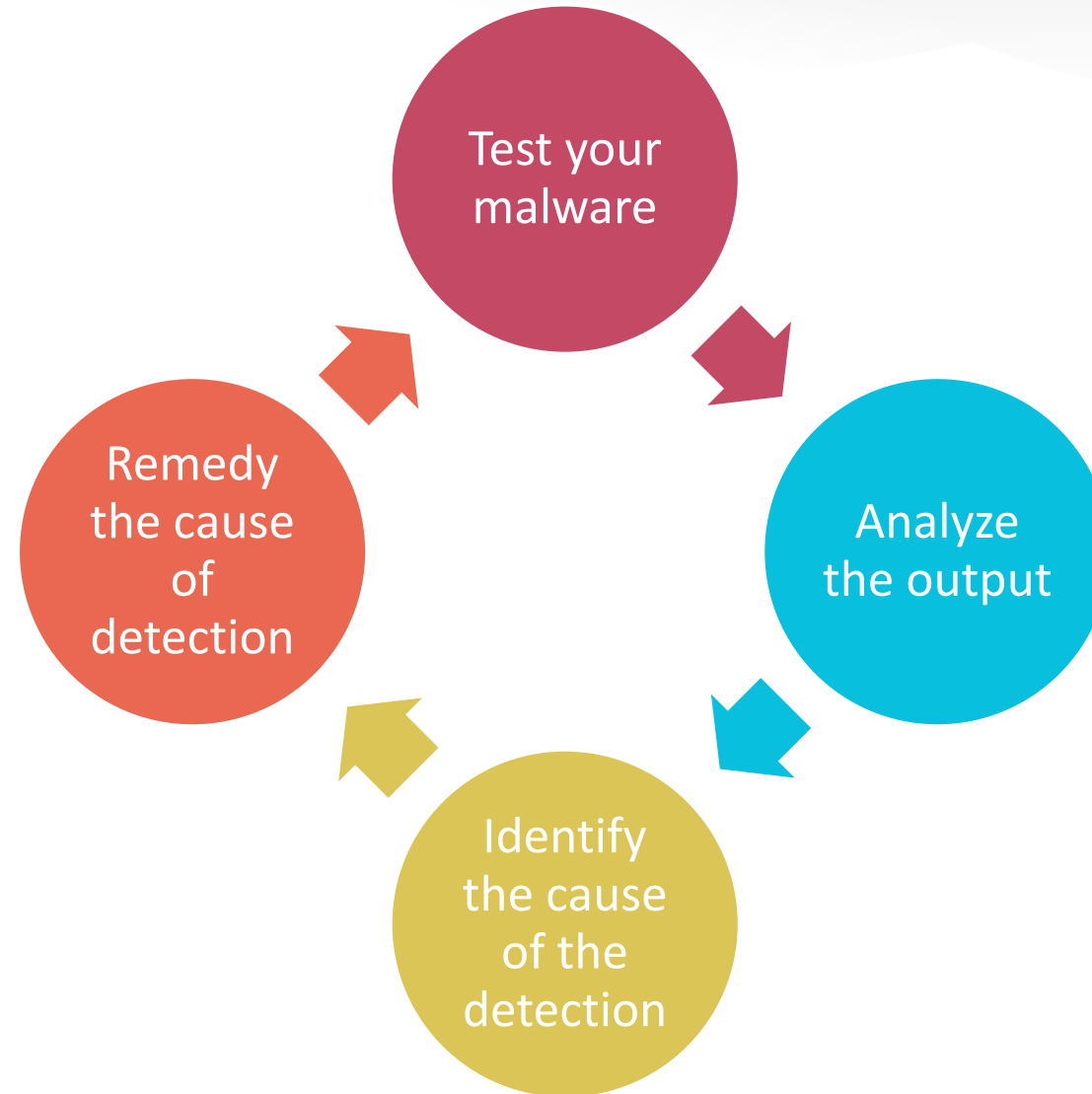

























Advertisement






Exploitation

# How to use a report to improve one's malware?



AV	Detection
 360 Total Security Essential	Clean
 ALYac Internet Security	Clean
 AVG Anti-Virus	Clean
 Ad-Aware Antivirus	Clean
 AhnLab V3 Light	Clean
 Avast Antivirus	Clean
 Avira Internet Security	TR/Crypt.XPACK.Gen
 BitDefender Total Security	Clean
 BullGuard Internet Security	Clean
 ClamAV	
 DrWeb Antivirus	
 Emsisoft Anti-Malware	
 Eset NOD32 Antivirus	
 F-PROT Antivirus	
 F-Secure Anti-Virus	Clean
 Fortinet Antivirus	Clean
 G Data Internet Security	Clean
 IKARUS anti.virus	Clean
 K7 AntiVirus Premium	Clean
 Kaspersky Internet Security	Clean
 Malwarebytes Premium	Clean
 McAfee Endpoint Protection	Clean
 Norton Security	Clean

 Avast Antivirus	Clean
 Avira Internet Security	TR/Crypt.XPACK.Gen
 BitDefender Total Security	Clean



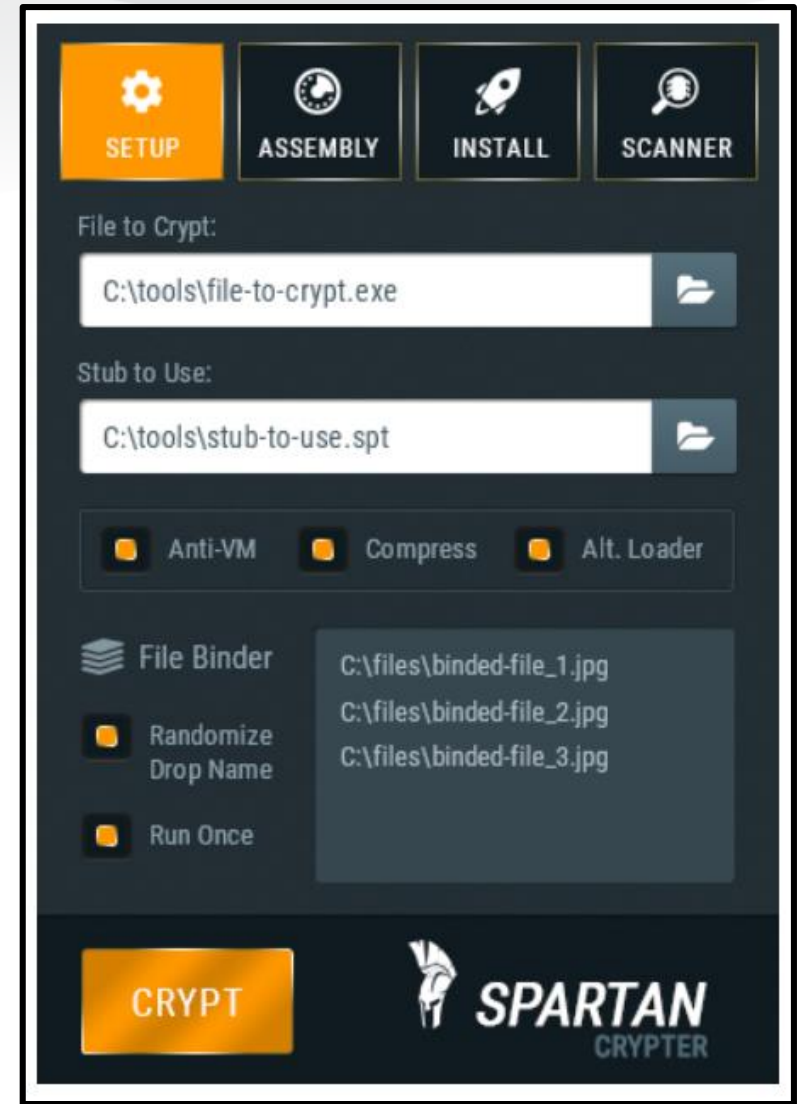
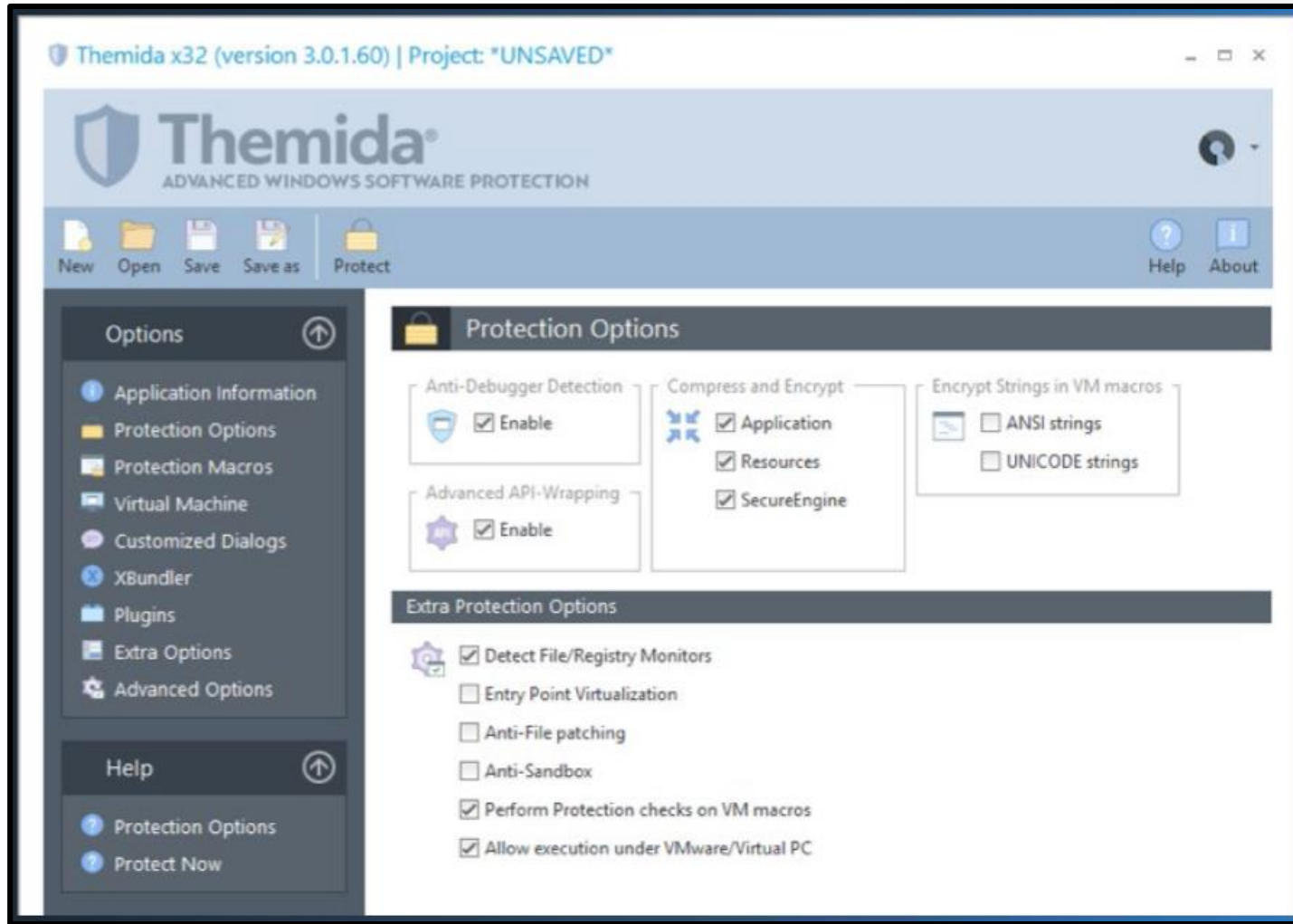
## From Avira's website:

“It **infects the MBR** (Master Boot Record) of the running system. If the Trojan is executed, it overwrites the MBR on the hard drive before the original MBR is stored in a second section”


“It makes a copy of itself in the following folder: **%Userprofile%\Local Settings\Temp\x2z8.exe**”

“Also, it drops a clean file in this folder: **%Userprofile%\Local Settings\Temp\fpah.txt**”


# Crypters



# Using an NDS to advertise your malware



monstercat  
Премиум  
Premium

Регистрация: 07.01.2019  
Сообщения: 38  
Реакции: 24  
Баллы: 10  
Jabber: 

11.11.2019

Актуальный на 12.11.2019 детект:  
Динчек: <https://dyncheck.com/scan/id/d099f03611a37d4939963885c9c698d8>  
Отстук (17/23): <http://prntscr.com/pvix0s>


Жалоба

Crypto Locker

КПОТ

Автор темы #37

Like + Цитата Ответ



Loliimbbb

Актуальные детекты:  
<https://www.scanlabs.net/user/result?id=1f2405e8cc1310e082c908e85a444507>

4 янв 2020

Borr

**DYNCHECK [01.05.2020]:**


Runtime FULL internet connection ( 9/23 ) - <https://dyncheck.com/scan/id/b24bf19633f278e24d5fac1311c3f3bb>

\*settings of this built: - Melt=OFF - Antidebug=ON - Install=ON - Start


\*Results may be better/worst with your crypter.

**PRICES:** - BOT 600\$ - STEALERS (Browsers, IM, Instants, FTP, RDP and web history) 100\$ - HIDDEN AMMY ADMIN 150\$ - REMOTE CONSOLE 100\$ - FILE STEALER 150\$ - KEYLOGGER 100\$ - RAM SCRAPER 250\$ - CRYPTO HIJACKER 100\$ - RANSOMWARE 500\$ - USB SPREAD 100\$ - BOLT 200\$ [Include updates]

DiamondFox



oski\_seller  
RAID-массив  
Пользователь

Регистрация: 30.10.2019  
Сообщения: 69  
Реакции: 22  
Баллы: 24  
Telegram: 

23.02.2020

Релиз Oski Stealer v7 fixed

Список изменений:

Билд:

- Переписан алгоритм шифрования строк внутри билда
- Убран мьютекс, сверяющий, запущена ли другая копия Oski в системе
- Переписан движок динамической подгрузки WinAPI
- Переработана работа со строками внутри билда

Актуальный рантайм:

Report #40cea2d1904177ccab31096683a71de0 | Dyncheck.com  
[dyncheck.com](https://dyncheck.com)

Oski Stealer — <https://xss.is/threads/32827/>

Жалоба

Like + Цитата Ответ

Oski

Автор темы #57

# Using an NDS to monitor the AV editor's response

## Periodic scans



2019 Dec 23 - Periodic Scan added

We have implemented period scan feature.  
It's available only to registered users.  
Feel free to try it.

## Domain check

### Update 1.3

In this update have been added

- Added new API
- Added URL AV/Blocklist checker (Available for paid users)
- For paid users, 2 APIs are available for checking files.
- In test mode, 2 free checks are available.\*

**RSA**Conference2020 **APJ**

---

A Virtual Learning Experience

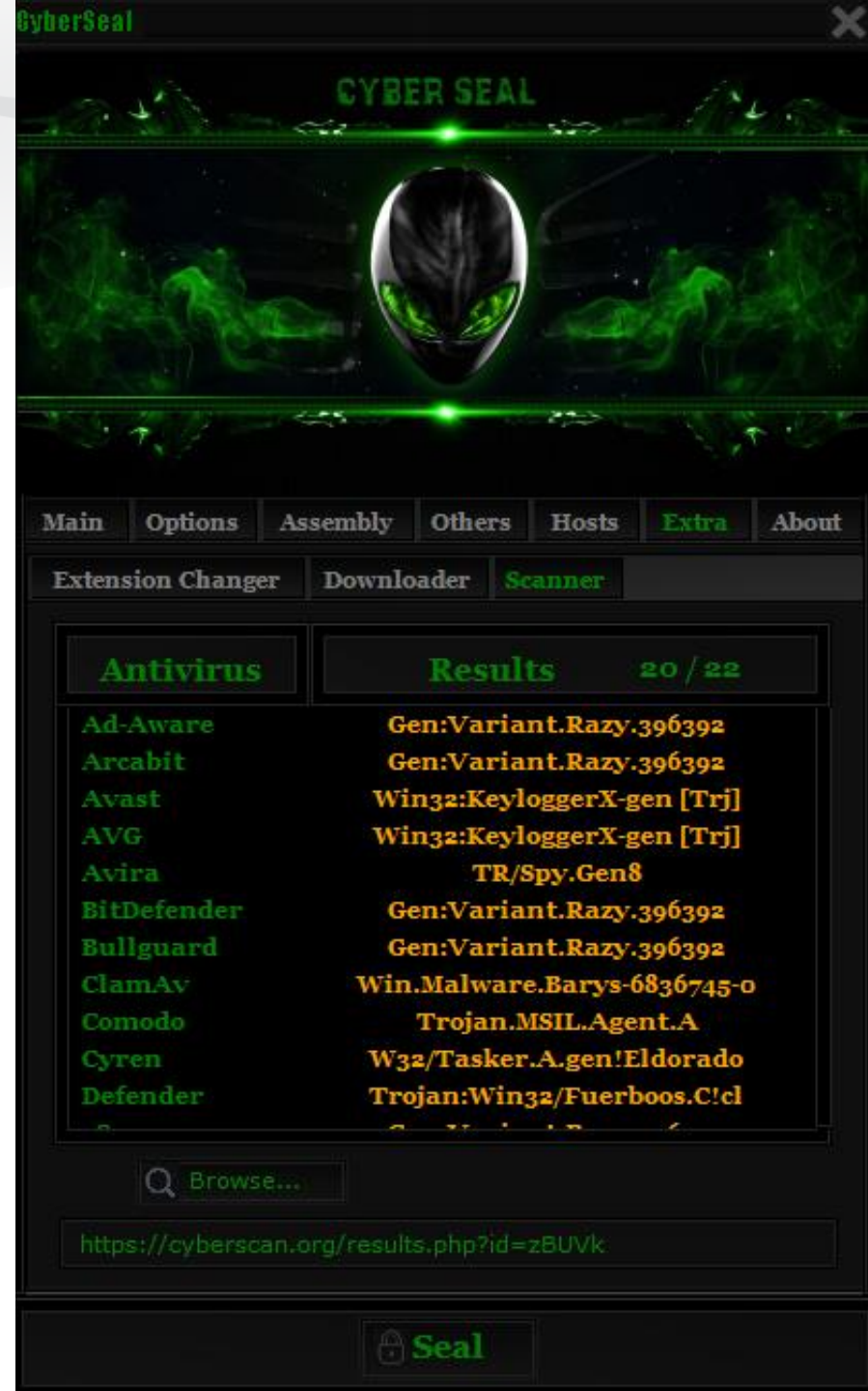
**NDS integrated into crimeware tools**

# NDS integrated in crypters

## Using an NDS API

- automation
- integration in other tools

```
#-----Edit only this-----  
//Set API key  
$api_key = "34836cf96c6d5b98b5fce482942761895c0df4f9";  
  
//Set API url  
$url_get_info = "https://dyncheck.com/api/get_info";  
#-----  
//File ID  
$file_id = $argv[1];  
  
//Generate JSON paramethres data  
$param_data = json_encode([  
    'api' => $api_key,  
    'file_id' => $file_id  
]);
```





# NDS being used by other NDS

Some NDS rely on another NDS for their backend:

**We at dyncheck.com would like to invite you to become a Partner Distributor of our service.**

*The major advantages for our Partner Distributors are:*

- ① dyncheck's loyal pricing leaves room for higher margins for the distributor (above 30%)
- ② Full cooperation and support from dyncheck. It varies depending upon our agreement type
- ③ Limited number of partner distributors.

If you are interested in becoming a partner distributor of dyncheck service, please write to us and we will shortly get in touch with you.

# **RSA**®Conference2020 **APJ**

---

A Virtual Learning Experience

## **Key Points**

# Key Points

- AV is not the panacea against malware
  - Antivirus doesn't stop all threats, and threat actors are monitoring what we're doing
- Monitoring the NDS landscapes allows us to identify important players and services in the cybercriminal ecosystem
  - Allows researchers & LE know where to invest resources
- Scan results shared by malware authors can help defenders identify and prioritize new and potent malware

**RSA**Conference2020 **APJ**

---

A Virtual Learning Experience

Questions?

**RSA**Conference2020 **APJ**

---

A Virtual Learning Experience

**Thank you!**

[mathieu.gaucheler@blueliv.com](mailto:mathieu.gaucheler@blueliv.com)

[liv.rowley@blueliv.com](mailto:liv.rowley@blueliv.com)