black hat USA 2017

JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

The Adventures of AV and the Leaky Sandbox

A **SafeBreach Labs** research by

Itzik Kotler, CTO and co-founder, SafeBreach

Amit Klein, VP Security Research, SafeBreach

SafeBreach

About Itzik Kotler

- 15+ years in InfoSec
- CTO & Co-Founder of **Safebreach**
- Presented in RSA, HITB, BlackHat, DEFCON, CCC, …
- http://www.ikotler.org

About Amit Klein

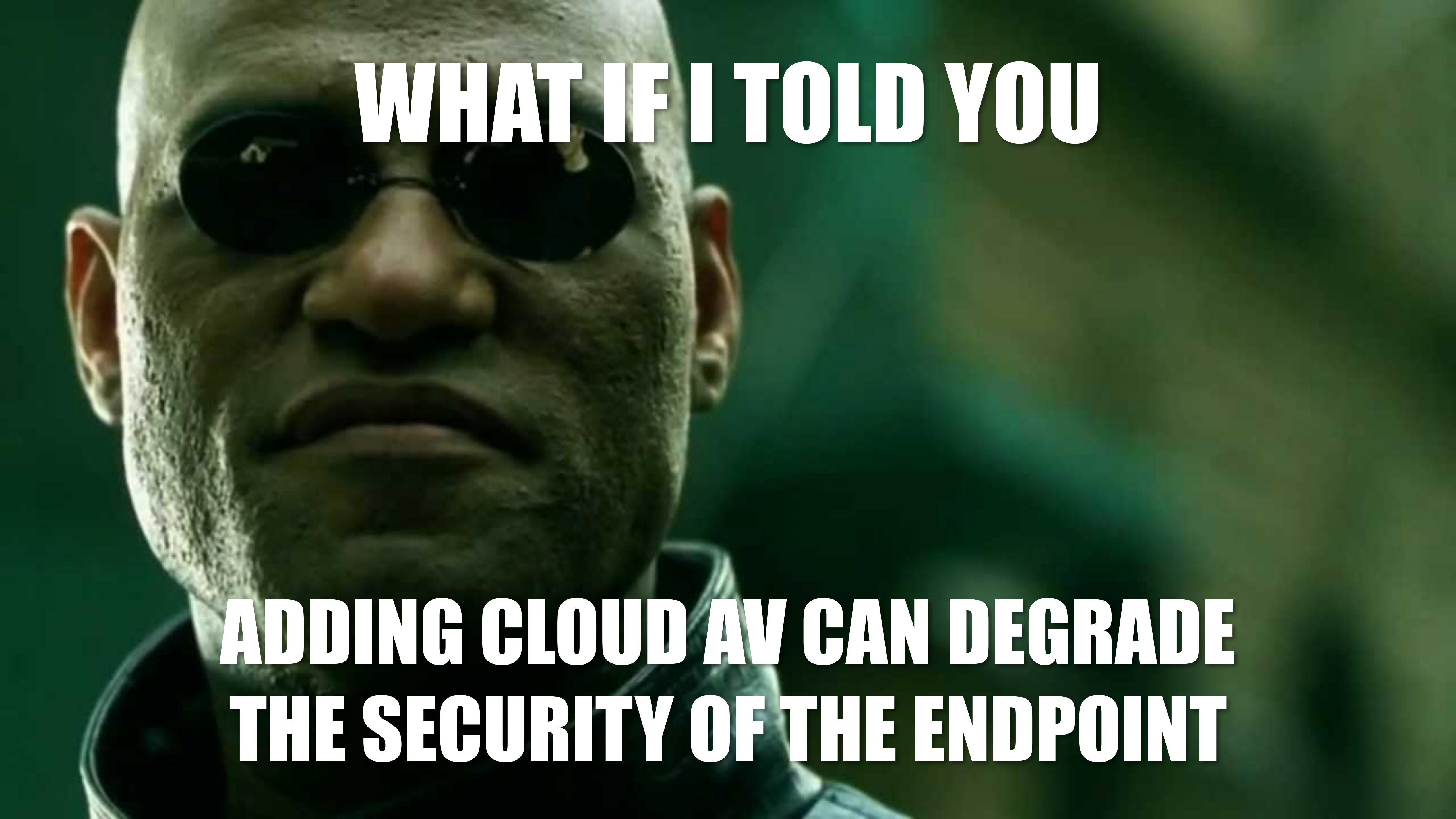
- 26 years in InfoSec
- VP Security Research **Safebreach** (2015-Present)
- 30+ Papers, dozens of advisories against high profile products
- Presented in BlackHat, HITB, RSA, CertConf, Bluehat, OWASP, AusCERT and more
- http://www.securitygalore.com

The story of the highly-secure enterprise

- **Variant #1: endpoints have restricted Internet access**
  - Software update servers (Microsoft Update)
  - AV update/services
- **Variant #2: endpoints have no direct Internet access**
  - On-premise update servers
  - On-premise AV management servers

Now let's throw in Cloud AV

- Everybody loves the "wisdom of clouds"
- What can possibly go wrong?



WHAT IF I TOLD YOU

ADDING CLOUD AV CAN DEGRADE
THE SECURITY OF THE ENDPOINT

Let’s degrade the security of the endpoint

- Assuming highly secure enterprise (=restricted/no direct Internet connection)
- We’re going to use the cloud AV to exfiltrate data from the endpoint
- Attacker can be anywhere in the Internet
- We’ll (ab)use the cloud AV sandbox

BUT FIRST –

RELATED WORK

Exfiltration at Large

Lots and lots of research on exfiltration techniques, e.g.:

- **“Covert Channels in TCP\IP Protocol Stack”** by Aleksandra Mileva and Boris Panajotov
- **“A survey of covert channels and countermeasures in computer network protocols”** by Sebastian Zander, Grenville Armitage and Philip Branch
- **“Covert timing channels using HTTP Catch Headers”** by Dennis Kolegov, Oleg Broslavsky and Nikita Oleksov

However, all practically assume unrestricted Internet connection

Exfiltration from air-gapped endpoints

Recent research on a more difficult scenario, e.g.:

- **“LED-it-GO Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED”** by Mordechai Guri, Boris Zadov, Eran Atias and Yuval Elovici
- **“Diskfiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise”** by Mordechai Guri, Yosef Solewicz, Andrey Daidakulov and Yuval Elovici
- **“BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations”** by Mordechai Guri, Matan Monitz, Yisroel Mirski and Yuval Elovici

All require an attacker in close proximity (not on the other side of the Internet)

Exfiltration via 3rd party sites

- **“Covert Communications Despite Traffic Data Retention”** by George Danezis – N/A since IP ID is no longer implemented as a global counter
- Piggybacking TCP SYN ISN/source port (with spoofed source IP) – egress filtering will kill it
- Piggybacking UDP source port/payload (with spoofed source IP) e.g. DNS – egress filtering will kill it
- **“In Plain Sight: The Perfect Exfiltration”** by Amit Klein and Itzik Kotler – AV services/SW update don’t have regular HTTP cache layer

Research on AV Sandboxes

Lots of AV sandbox fingerprinting/detection works:

- **“AVLeak: Fingerprinting Antivirus Emulators Through Black-Box Testing”** by Jeremy Blackthorne, Alexei Bulazel, Andrew Fasano, Patrick Biernat and Bülent Yener
- **“Your sandbox is blinded: Impact of decoy injection to public malware analysis systems”** by Katsunari Yoshioka, Yoshihiko Hosobuchi, Tatsunori Orii and Tsutomu Matsumoto
- **“Enter Sandbox – part 8: All those… host names… will be lost, in time, like tears… in… rain”** by Hexacorn Ltd.

Research on AV Sandboxes (continued)

- **“Sandbox detection: leak, abuse, test”** by Zoltan Balazs
- **“Art of Anti Detection 1 – Introduction to AV & Detection Techniques”** by Ege Balci

They all leak info from the sandbox, but they don’t leak info from the endpoint!

Research on AV Sandboxes (continued)

Leaking data from an endpoint (≠ cloud) sandbox, assuming direct (unrestricted) Internet access from the endpoint

- Google’s Project Zero entry **“Comodo: Comodo Antivirus Forwards Emulated API calls to the Real API during scans”** by Tavis Ormandy

EXFILTRATION VIA A CLOUD AV SANDBOX

Let’s do it already

BUT FIRST –

TWO BASIC TECHNIQUES

#1: Triggering an AV event

Numerous ways, a comprehensive list in **“Art of Anti Detection 1 – Introduction to AV & Detection Techniques”** by Ege Balci.

We’ll use only two very simple triggers:

- Writing the EICAR file to disk
- Installing the “malware” (persistence) by moving its binary under the Windows Startup folder

#2: Exfiltration from an Internet-connected machine

Numerous ways (see earlier “Exfiltration at large” slide)

We’re going to use:

- Sending HTTP/HTTPS request to the attacker’s host
- Forcing DNS resolution

EXFILTRATION VIA A CLOUD AV SANDBOX

Are we there yet?

Assumptions on the AV and the attacker’s malware

- An AV product (agent) installed on endpoints, which submits to the AV cloud unknown/suspicious executable files:
  - Directly
  - Indirectly
- The AV cloud service employs a sandbox which can directly connect to the Internet.
- The attacker’s process (malware) is running on the endpoint.

ATTACK FLOW

Attack Components

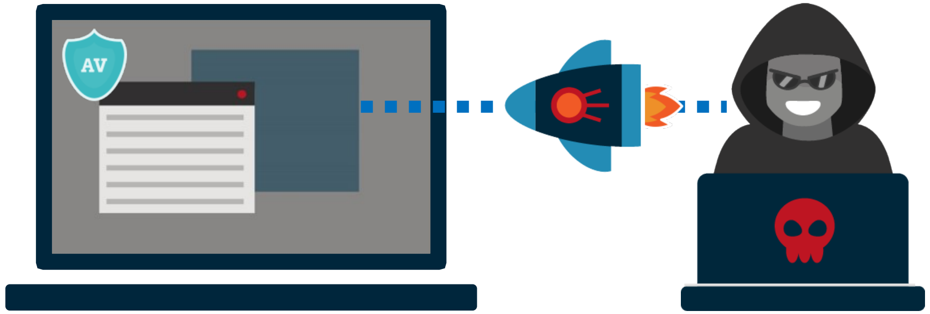
Rocket

The *Rocket* is the main attacker malware, responsible for sensitive data collection (which becomes the payload for exfiltration). The Rocket contains a "vanilla" copy of another malware executable, called Satellite.

Satellite

The *Satellite* is the secondary malware executable, which triggers the AV agent and later conducts the actual exfiltration.

0. The Attacker infects the endpoint with the Rocket

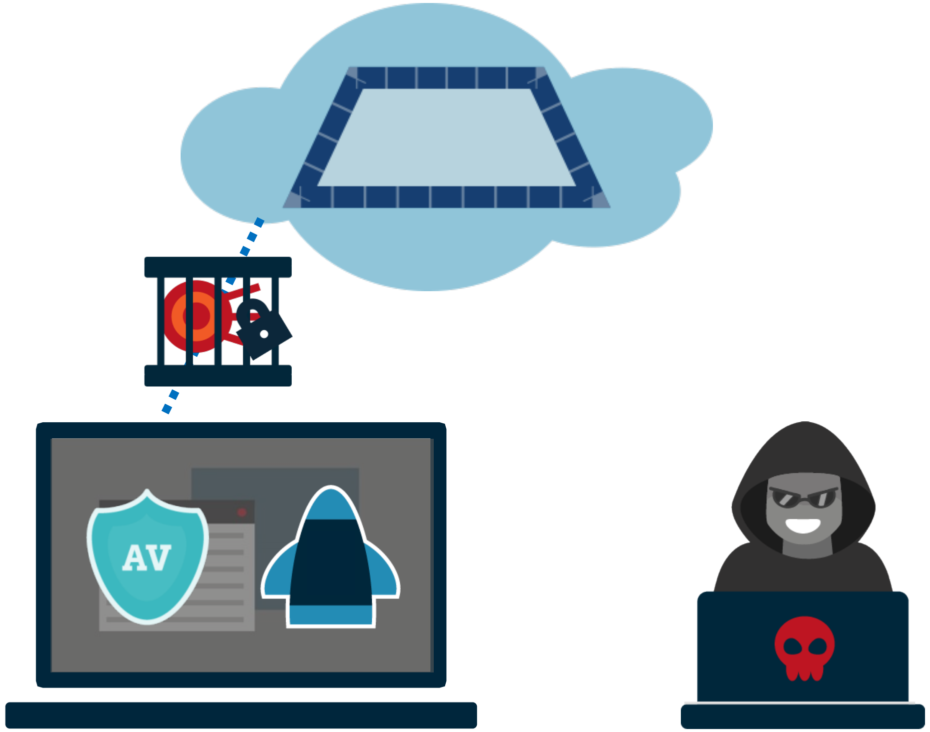


1. The Rocket collects sensitive data from the endpoint and embeds it into the Satellite

2. The Rocket writes the Satellite to disk and executes it

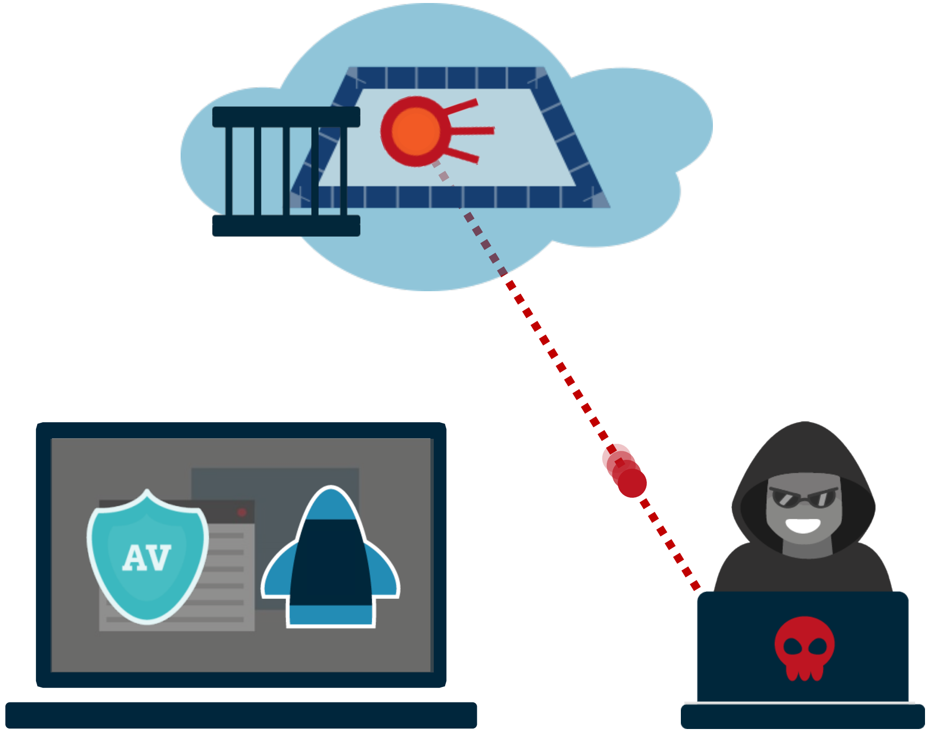
3. The Satellite triggers the AV agent

4. The AV agent sends the Satellite to the AV cloud service for further inspection

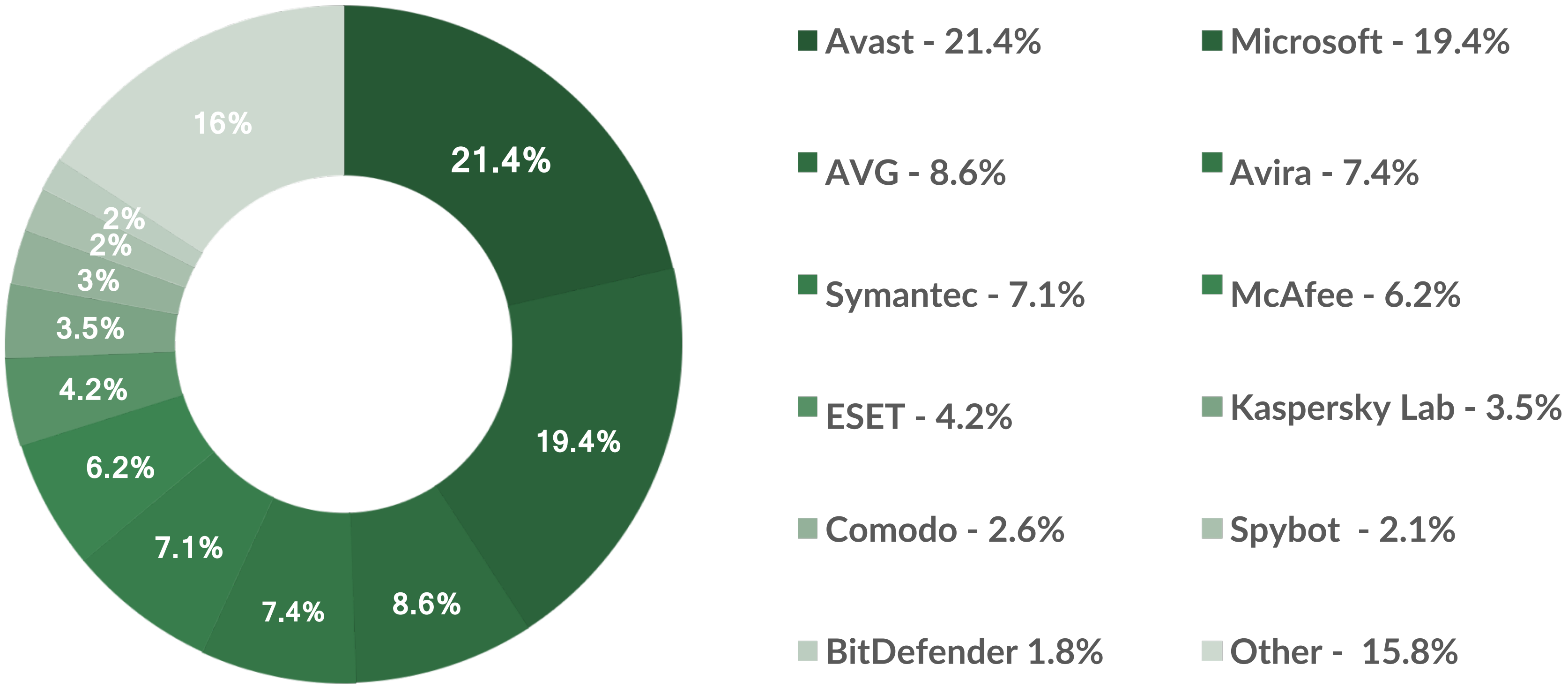


5. The AV cloud service executes the Satellite in a sandbox

6. The Satellite sends the collected data over the internet to the attacker



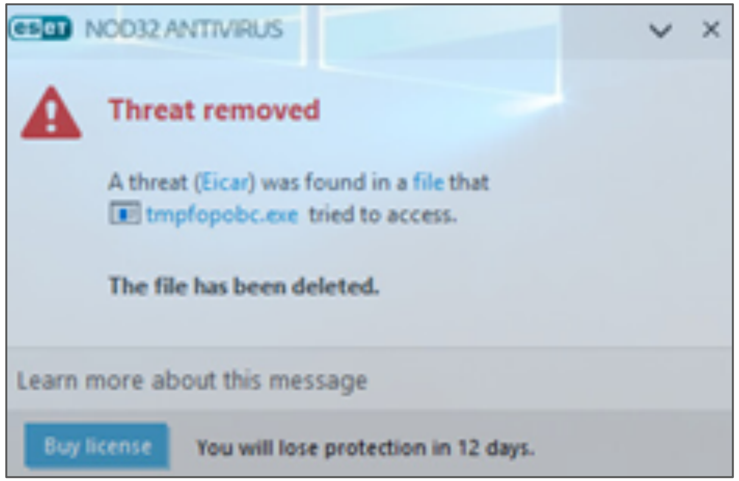
OPSWAT'S "most recent" AV market share



Results with leading AV Products

Product	Version	Trigger	Exfil. method	Success
Avast Free Antivirus	12.3.2280			-
Microsoft Windows Defender	Client v. 4.10.14393.0 Engine v. 1.1.13407.0			-
AVG	Build 1.151.2.59606 Framework v. 1.162.2.59876			-
Avira Antivirus Pro	15.0.25.172	Persistence	DNS, HTTP	Yes
Symantec Norton Security	22.8.1.14			-
McAfee Cloud AV	0.5.235.1			-
ESET NOD32 Antivirus	10.0.390.0	EICAR	DNS	Yes
Kaspesrky Total Security 2017	17.0.0.611(c)	Persistence	DNS, HTTP	Yes
Comodo Client Security	8.3.0.5216	Persistence	DNS, HTTP	Yes
BitDefender Total Security 2017	Build 21.0.23.1101 Engine v. 7.69800			-

It’s not too subtle (but who cares?)



ESET NOD32 ANTIVIRUS

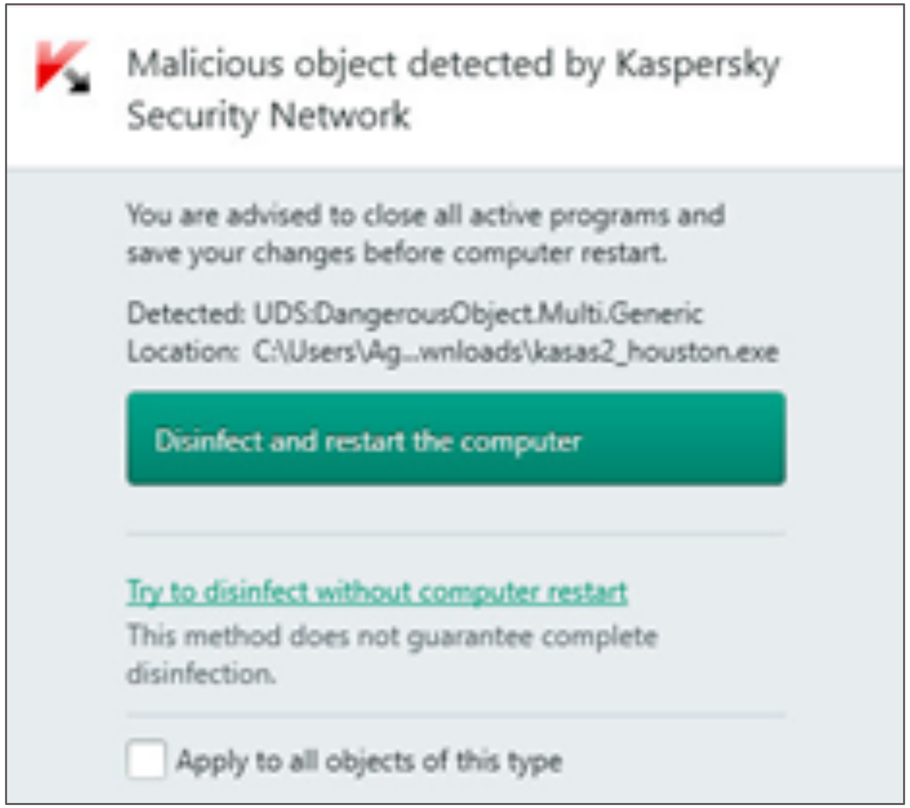
Threat removed

A threat (Eicar) was found in a file that tmpfopobc.exe tried to access.

The file has been deleted.

Learn more about this message

You will lose protection in 12 days.



Malicious object detected by Kaspersky Security Network

You are advised to close all active programs and save your changes before computer restart.

Detected: UDS:DangerousObject.Multi.Generic
Location: C:\Users\Ag...wnloads\kasas2_houston.exe

Try to disinfect without computer restart

This method does not guarantee complete disinfection.

□ Apply to all objects of this type

Insights on cloud AV sandboxes

- Some sandboxes (ESET) blocked HTTP (but not DNS)
- Some sandboxes blocked access to the environment variables
- Some have non-standard software and environment variables
- Cloud AV sandboxes are easily detectable
    - Computer name
    - Disk volume serial number
    - MAC address
    - Performance counter frequency

Insights on cloud AV sandboxes (continued)

- Some sandbox infrastructure is shared among several vendors
- Lead time varies wildly – minutes to hours
- Multiple executions
- Binary extraction and execution of the Satellite (from the Rocket)

Cloud AV sandbox sample names

- **ESET:** REYNAPC, MALVAPC, ELEANOREPC, WRIGHTPC, BRIAPC, JORIPC, GABBIPC, HELSAPC, MAMEPC, SHARAIPC, ARACHONPC, FLORIANPC, EDITHPC
- **Various:** WIN7-PC, ROGER-PC, DAVID-PC, ADMIN-PC, APIARY7-PC, ANTONY-PC, LUSER-PC, PERRY-PC, KLONE_X64-PC, 0M9P60J5W-PC, MIKI-PC
- **Avira:** C02TT22, C02TT26, C02TT36, C02TT18, C06TT43
- **Comodo:** spurtive, circumstellar
- **Others:** ZGXTIQTG8837952 (**Comodo**), ABC-WIN7, PC, WIN-U9ELNVPPAD0, PC-4A095E27CB, WIN-LRG949QLD21

(in blue – names found in the 2015 Hexacorn list – 7/37)

ZGXTIQTG8837952 (**Comodo**)

```
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\Administrator\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=FS02
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\Administrator
LOCALAPPDATA=C:\Users\Administrator\AppData\Local
LOGONSERVER=\\FS02
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Wi
ndows\System32\WindowsPowerShell\v1.0\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3,
GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=3c03
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=$P$G
PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\ADMINI~1\AppData\Local\Temp
tHH=12
tMM=32
TMP=C:\Users\ADMINI~1\AppData\Local\Temp
tmpH=12
tmpM=29
tmpS=16
tnext=45158
tnow=44956
tSS=38
USERDOMAIN=FS02
USERNAME=BLtJc5wjxpj53
USERPROFILE=C:\Users\BLtJc5
windir=C:\Windows
windows_tracing_flags=3
windows_tracing_logfile=C:\BVTBin\Tests\installpackage\csilogfile.
log]
```

A less obvious fingerprint

- Obvious fingerprints: MAC address, disk volume number, domain
- Environment variable names can be easily detected
- Values have easily detectable relations
  - `tmpH=12 tmpM=29 tmpS=16` → 12:29:16 = Now (UTC-0700)
  - `tnow=44956` = Now (UTC-0700) in seconds since midnight
  - `tHH=12 tMM=32 tSS=38` → 12:32:38 = Now+202s (UTC-0700)
  - `tnext=45158` = Now+202s (UTC-0700) in seconds since midnight

On-Premise AV Sandboxes

- A more secure alternative to cloud AV sandboxes
- Same attack technique may apply, depending on:
  - Outbound traffic **sandbox** network policy
  - Outbound traffic **enterprise** network policy
- We did not test this, but we speculate that vulnerable combinations do occur at a non-negligible portion of the installations

Sample sharing considered harmful

Any sample sharing outside the enterprise (or even inside) can facilitate exfiltration:

- Security mailing lists
- File/sample repositories
- Expert analysis services

Online/cloud sandbox/scanning services

- When used as a 3rd party detection/classification engine
- When used manually!

Exfiltration demonstrated possible with:

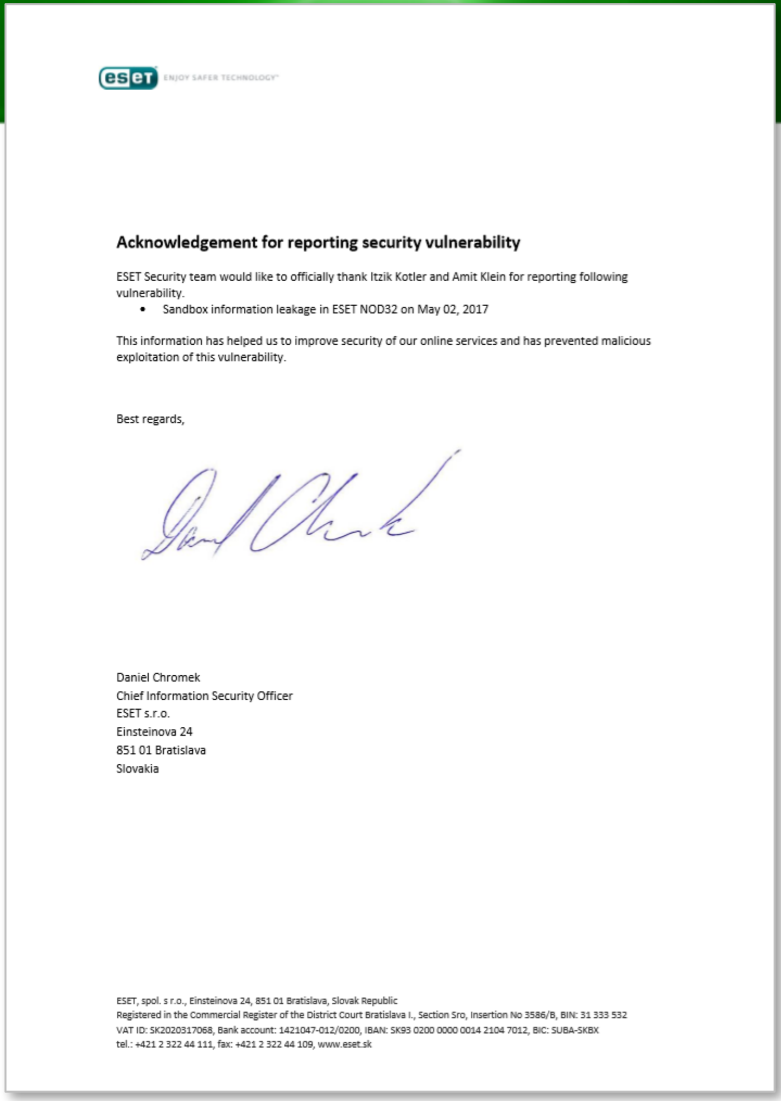
- **Google VirusTotal** (www.virustotal.com)
- Joe Security **Joe Sandbox Cloud** (www.file-analyzer.net) – only DNS, limited to 10 queries
- Payload Security **Hybrid Analysis** (www.reverse.it)

Demo time

Latest code and slides can always be found at: https://github.com/SafeBreach-Labs/spacebin

Vendor status – cloud AV

- **Avira** – fixed on May 2nd (10h30m!)
- **ESET** – fixed on May 15th or before
- **Comodo** – fixed on May 26th
- **Kaspersky** - provided to us on July 14th with the following statement: *"If customers are concerned about this scenario, they may configure their device and security settings accordingly. Those using our consumer products can disable files sent to the cloud sandbox without affecting detection effectiveness. Those using corporate products can install Kaspersky Private Security Network, the on-premises version of the Kaspersky Security Network cloud service, or a private fix to disable files sent to the cloud sandbox."*



ESET ENJOY SAFER TECHNOLOGY™

Acknowledgement for reporting security vulnerability

ESET Security team would like to officially thank Itzik Kotler and Amit Klein for reporting following vulnerability.

- Sandbox information leakage in ESET NOD32 on May 02, 2017

This information has helped us to improve security of our online services and has prevented malicious exploitation of this vulnerability.

Best regards,

Daniel Chromek
Chief Information Security Officer
ESET s.r.o.
Einsteinova 24
851 01 Bratislava
Slovakia

ESET, spol. s r.o., Einsteinova 24, 851 01 Bratislava, Slovak Republic
Registered in the Commercial Register of the District Court Bratislava I., Section Sro, Insertion No 3586/B, BIN: 31 333 532
VAT ID: SK2020317068, Bank account: 1421047-012/0200, IBAN: SK93 0200 0000 0014 2104 7012, BIC: SUBA-SKBX
tel.: +421 2 322 44 111, fax: +421 2 322 44 109, www.eset.sk

Vendor status – cloud sandboxes

- **VirusTotal** – informed us on June 16th that they WONTFIX, and provided the following statement: *“We have our sandboxes on the internet on purpose to allow them communicate with C2 machines so we record the traffic”*
- **Joe Security** – fixed on June 19th (3d11h!)

  “Improved ISIM max UDP request config (@credits to Amit & Itzik from Safebreach)”
- **Payload Security** - informed us on June 23rd that "*Payload Security chooses not to comment*".

Suggested improvements for cloud AVs

- Block all traffic to the Internet from the sandbox
- Only allow a sample to Interact with the Internet if the sample arrives from the Internet
    - Must be byte-wise identical to the copy arriving from the Internet
    - Not enough for the copy to arrive from “elsewhere”
    - Not applicable to standalone cloud scanners/analyzers (e.g. VirusTotal)

Future research directions

- Additional triggers
- Additional exfiltration methods (e.g. SMTP, IRC, ICMP)
- Encrypting/compressing the Satellite template (inside the Rocket)
- Simulating AV agent-cloud protocol for stealthier exfiltration

Conclusions / take-aways

- AVs using **Internet-connected sandboxes** can facilitate exfiltration even from highly secure enterprises
  - In-the-cloud sandbox
  - On-premise sandbox
- Sharing suspicious/malicious files can facilitate exfiltration, unless the file has arrived from outside the enterprise and is unmodified.
  - Online/cloud scanning/analysis services (VirusTotal, etc.)
  - Any sample sharing at large
- Avira, ESET and Comodo fixed their sandboxes, so are probably safe. Kaspersky is vulnerable unless its users switch off the cloud sample submission feature. Other vendors' status is unclear.

Acknowledgement

Thanks to Yoni Fridburg – for his help in setting up the AV research lab

SafeBreach

Thank You!

Questions?