The development of a contained and user emulated malware assessment platform

Siebe Hodzelmans & Frank Potter

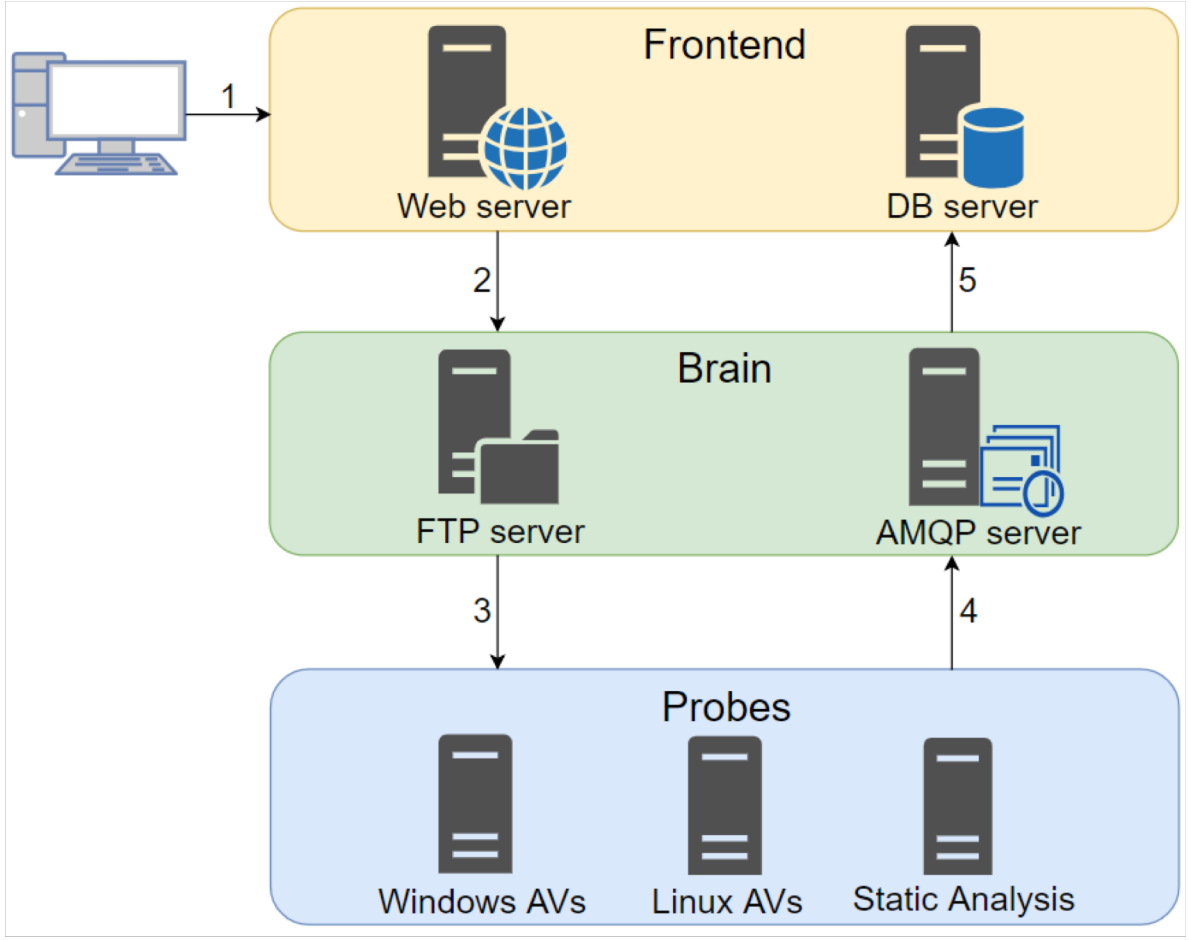
Google Acquires Online Virus, Malware and URL Scanner VirusTotal

Frederic Lardinois @fredericl / 6 years ago

VirusTotal, an online malware and virus scanner, was just acquired by Google. The company already used a number of **Google** services ahead of the acquisition, including App Engine and Google Storage. VirusTotal will continue to operate

(TechCrunch, 2012)

Incident Response and Malware Analysis



(Debrie, Lone-Sang, and Quint, 2014)

Kaspersky: Yes, we obtained NSA secrets. No, we didn't help steal them

Moscow-based AV provider challenges claims it helped Russian spies.

DAN GOODIN - 11/16/2017, 11:00 AM

(ArsTechnica, 2017)

What Do Antivirus's Actually Do?

TECH

JANUARY 31, 2019

Antivirus software is one of those things we can often take for granted. Many people have a "set it and forget it" approach to their antivirus settings. Or they may be under the misconception that antivirus software simply scans your files for viruses.

(Times Square Chronicles, 2019)

Research question

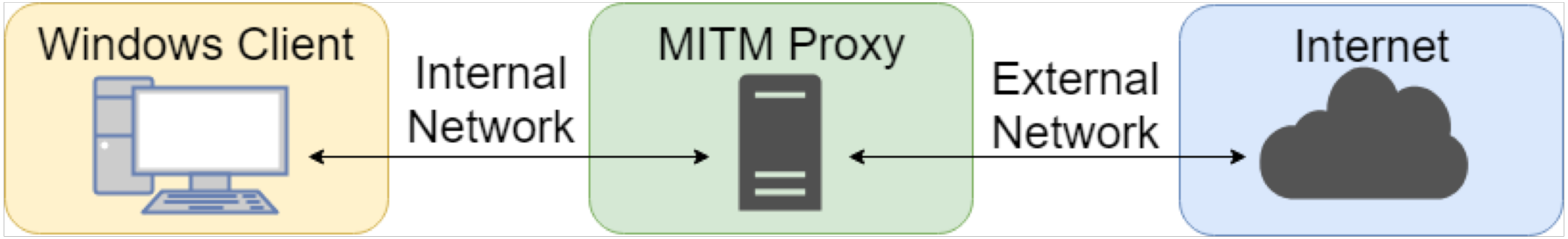
‘How can malware be tested for detection of antivirus software by emulating user actions, without the AV vendor learning about the malware?’

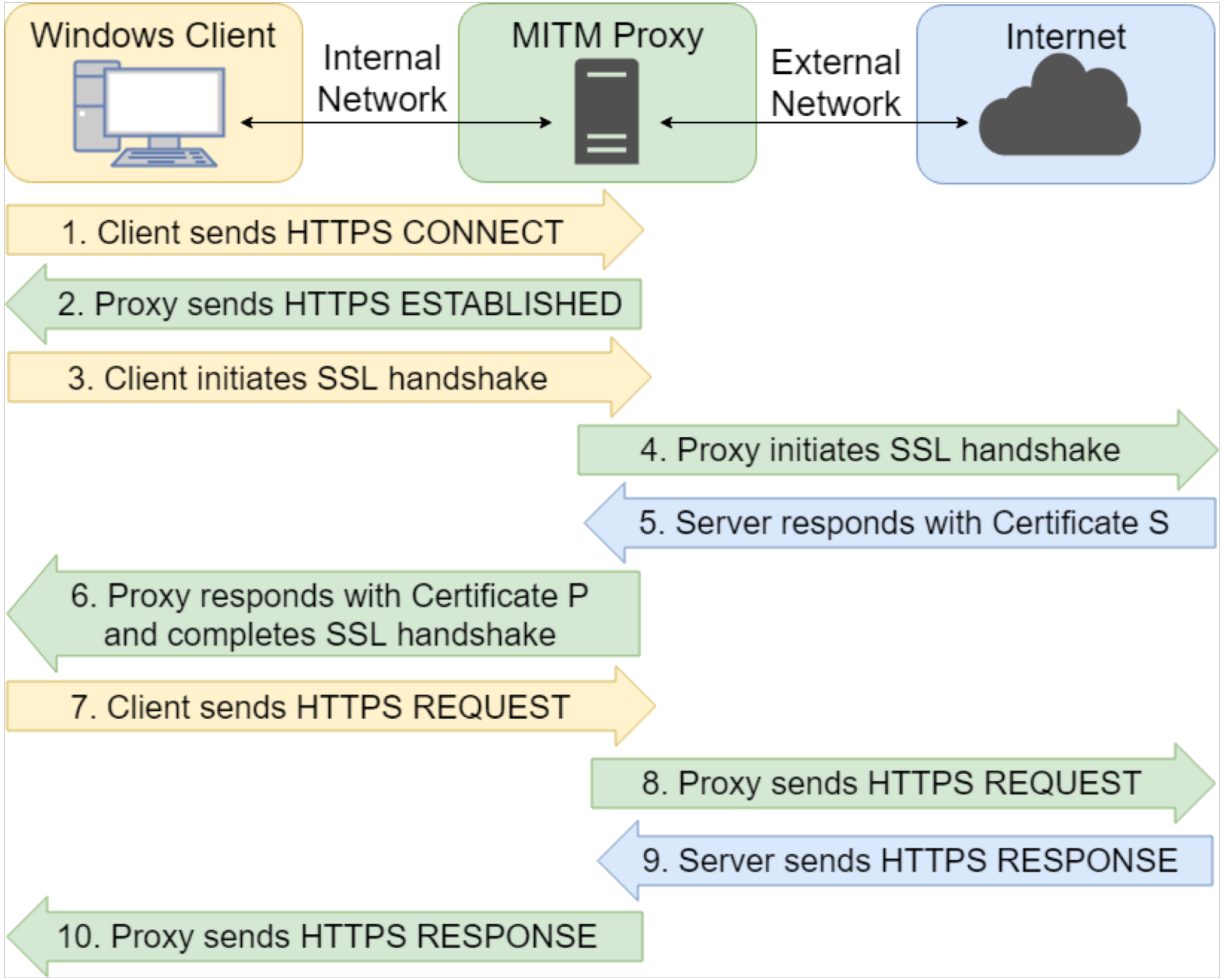
Sub questions

- What traffic is generated by AV software?
- How to prevent AV software from notifying and submitting the red team's malware to the AV vendor?
- Are there any differences between direct scanning and user emulated detection rates?

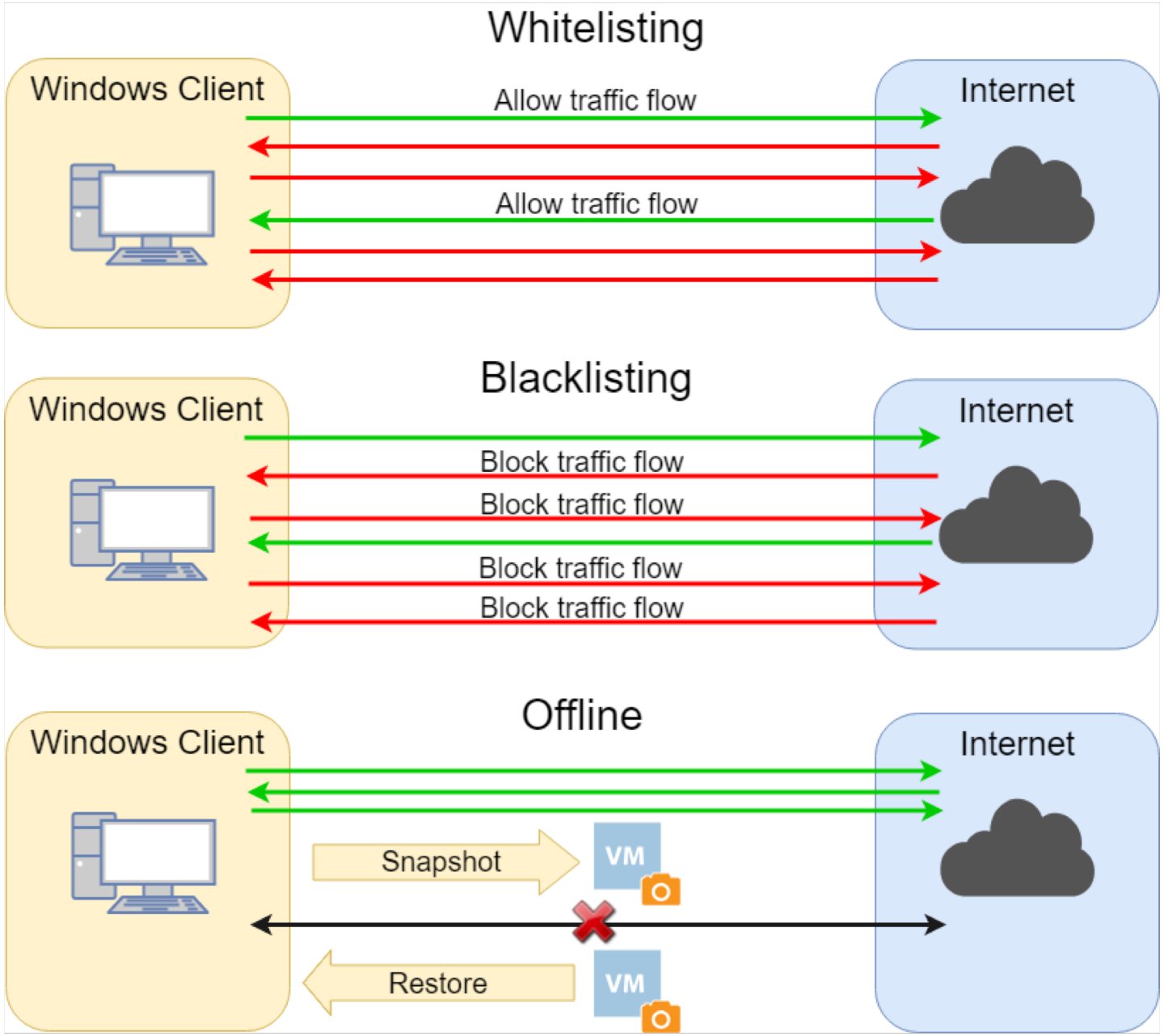
Methodology - Traffic analysis

- McAfee, Symantec and Trend Micro
- Malware samples



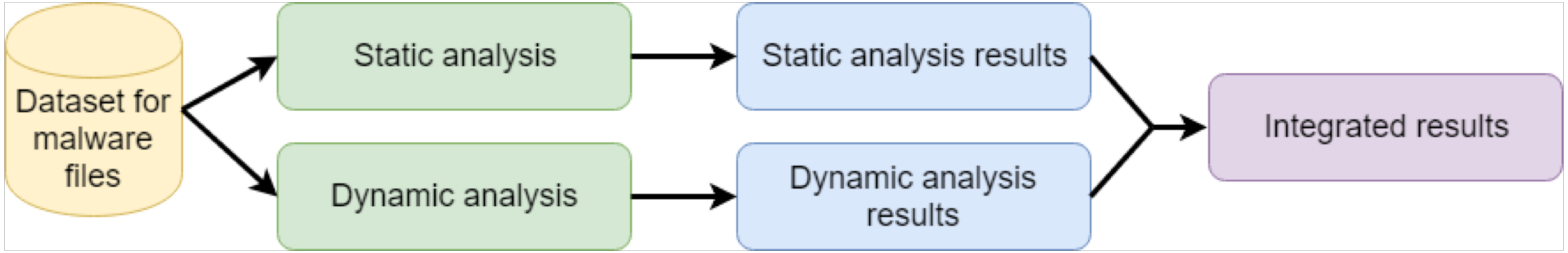

Windows Client
Internal Network
MITM Proxy
External Network
Internet
1. Client sends HTTPS CONNECT
2. Proxy sends HTTPS ESTABLISHED
3. Client initiates SSL handshake
4. Proxy initiates SSL handshake
5. Server responds with Certificate S
6. Proxy responds with Certificate P and completes SSL handshake
7. Client sends HTTPS REQUEST
8. Proxy sends HTTPS REQUEST
9. Server sends HTTPS RESPONSE
10. Proxy sends HTTPS RESPONSE

Methodology - Preventing submission


Whitelisting
Windows Client
Allow traffic flow
Internet
Allow traffic flow
Blacklisting
Windows Client
Internet
Block traffic flow
Block traffic flow
Block traffic flow
Block traffic flow
Offline
Windows Client
Internet
Snapshot
VM
Restore
VM

Methodology - User emulation

- Compare manual with emulated behavior of malware
- Web browsing user emulation with pywinauto and pyautogui
- Malware infection Tree



(Kamali, 2016)

Results - Traffic analysis

- Traffic capture:
  - McAfee, Symantec and Trend Micro
  - Later Kaspersky

- In general:
  - Installation, registration, updating
  - Analytical data
  - Lots of hashes and encoded data
  - Only HTTP(S)

Results - Traffic analysis

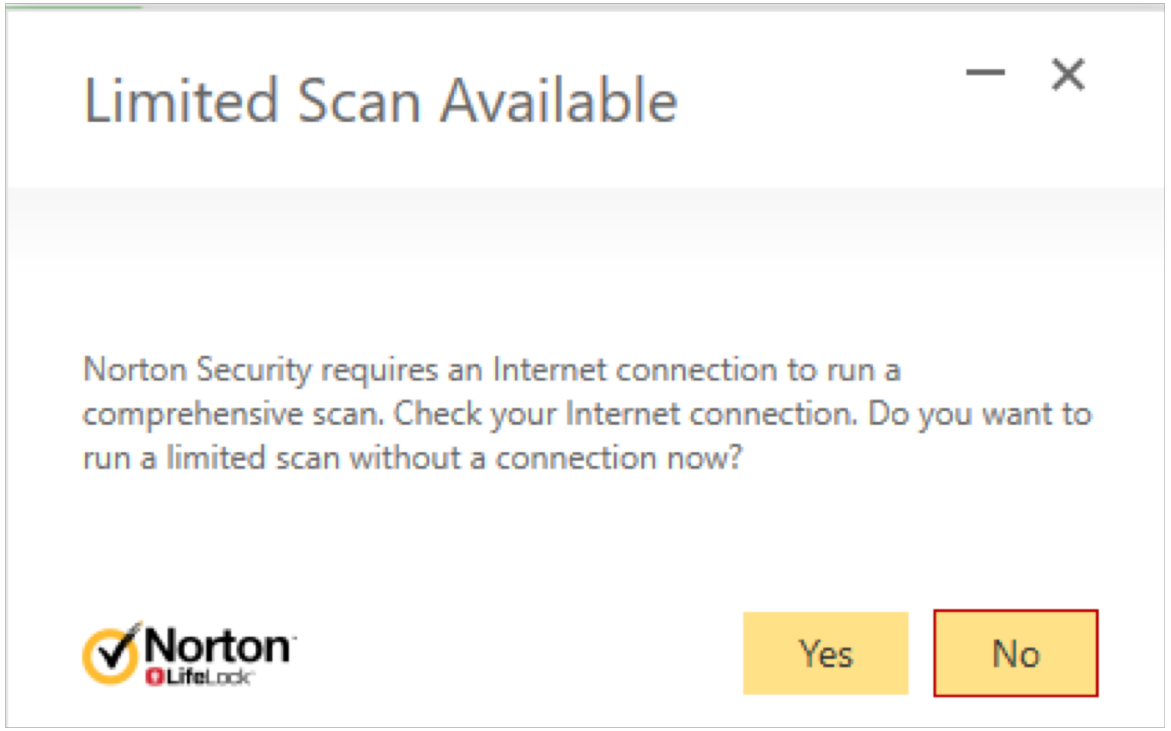
- Noteworthy:
  - Trend Micro: missing SNI, long plain HTTP GET
  - McAfee: every file gets hashed, google analytics
  - Symantec: ping submission with data buffer
  - Kaspersky: lot of HTTP(S) 400 and 502 errors, certificate pinning
- No sample submission

Results - Traffic analysis

	Das Malwerk					Deloitte obfuscated			Deloitte direct exports		
	1e84-ff45	1f7b-55c7	230a-6f87	266a-11f5	2578-6c51	obf. exe	obf. dll 1	obf. dll 2	beacon exe	beacon dll	msf vnm
McAfee	✓	✓							✓	✓	✓
Symantec	✓	✓	✓	✓	✓				✓	✓	✓
Trend Micro	✗ ✓	✓	✓	✓	✓						✓
Kaspersky	✓	✓	✓	✓	✓				✓	✓	✓

Results - Sample submission prevention

- Offline: undesirable
  - Difference Trend Micro
  - Warning Symantec
- Blacklisting
  - Unsure what to block
  - Updates can change endpoints
- Whitelisting
  - Robust
  - Parameters:
    - hostnames
    - traffic size and direction
    - content



Results - User emulation

- Two ways:
  - pywinauto, accessibility API
  - pyautogui, mouse and keyboard, screenshots
- Compared manual to emulation
  - Malware infection Tree
  - File handles, process tree structure

Win32.WannaPeace.exe	244		
newstar.exe	3276		
conhost.exe	5296	Console Window Host	Microsoft Corporation
netsky4.exe	7184		
conhost.exe	4500	Console Window Host	Microsoft Corporation
cmd.exe	5356	Windows Command Processor	Microsoft Corporation
conhost.exe	5808	Console Window Host	Microsoft Corporation
DePass_Micro.exe	308	DePass Micro	Kalyuk Vitaliy (KVSoft Ukraine)

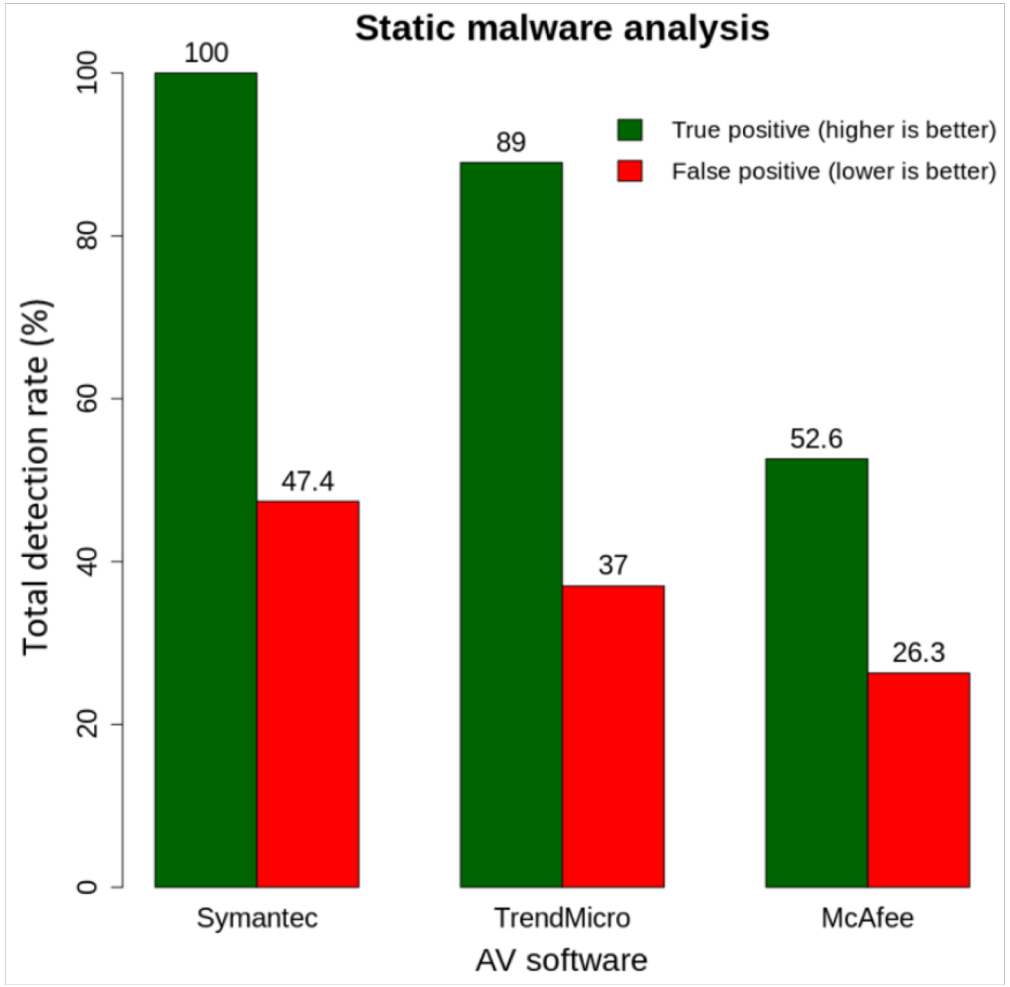
Win32.WannaPeace.exe	4696		
newstar.exe	2856		
conhost.exe	4872	Console Window Host	Microsoft Corporation
netsky4.exe	3448		
conhost.exe	5136	Console Window Host	Microsoft Corporation
cmd.exe	5536	Windows Command Processor	Microsoft Corporation
conhost.exe	2336	Console Window Host	Microsoft Corporation
DePass_Micro.exe	6908	DePass Micro	Kalyuk Vitaliy (KVSoft Ukraine)

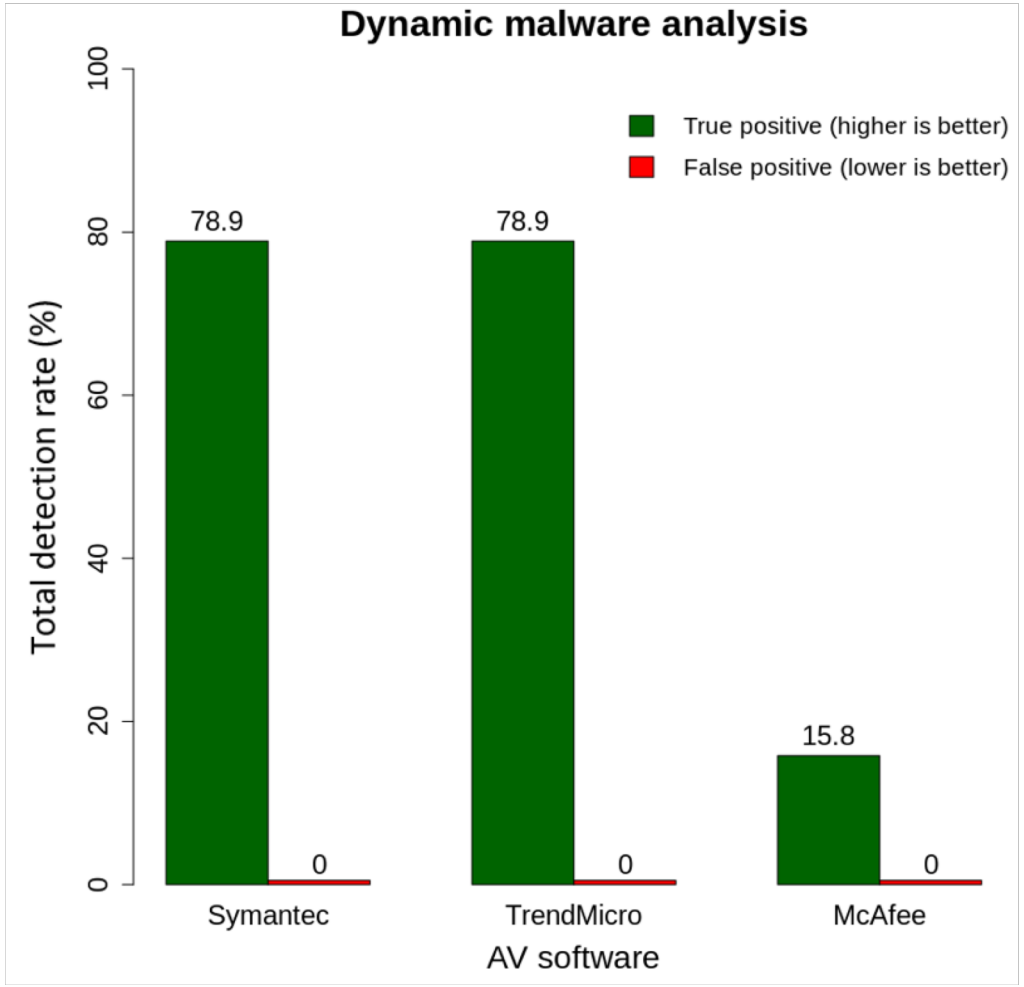
Results - User emulation

Time ...	Process Name	PID	Operation	Path	Result
16:39:...	Win32.WannaPeace....	3936	Process Start		SUCCESS
16:39:...	Win32.WannaPeace....	3936	Thread Create		SUCCESS
16:39:...	Win32.WannaPeace....	3936	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
16:39:...	Win32.WannaPeace....	3936	ReadFile	C:\ProgramData\Norton\{0...	SUCCESS
16:39:...	Win32.WannaPeace....	3936	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
16:39:...	Win32.WannaPeace....	3936	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
16:39:...	Win32.WannaPeace....	3936	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
16:39:...	Win32.WannaPeace....	3936	ReadFile	C:\ProgramData\Norton\{0...	SUCCESS
16:39:...	Win32.WannaPeace....	3936	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
16:39:...	Win32.WannaPeace....	3936	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
16:39:...	Win32.WannaPeace....	3936	Load Image	C:\Users\RP1\Downloads\...	SUCCESS

Time ...	Process Name	PID	Operation	Path	Result
13:37:...	Win32.WannaPeace....	6776	Process Start		SUCCESS
13:37:...	Win32.WannaPeace....	6776	Thread Create		SUCCESS
13:37:...	Win32.WannaPeace....	6776	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
13:37:...	Win32.WannaPeace....	6776	ReadFile	C:\ProgramData\Norton\{0...	SUCCESS
13:37:...	Win32.WannaPeace....	6776	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
13:37:...	Win32.WannaPeace....	6776	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
13:37:...	Win32.WannaPeace....	6776	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
13:37:...	Win32.WannaPeace....	6776	ReadFile	C:\ProgramData\Norton\{0...	SUCCESS
13:37:...	Win32.WannaPeace....	6776	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
13:37:...	Win32.WannaPeace....	6776	QueryStandardInformation...	C:\ProgramData\Norton\{0...	SUCCESS
13:37:...	Win32.WannaPeace....	6776	Load Image	C:\Users\RP1\Downloads\...	SUCCESS

Results - User emulation





Discussion

- Contamination of packet captures
- mitmproxy
  - Insecure connections
  - Kaspersky errors
- Results of sample submission prevention
  - Unable to trigger sample submission
  - Flaw in research design
  - Based on what we did observe
- McAfee low detection rate

Conclusion

- Variety of traffic
  - But no sample submission
- Whitelisting the best approach
- Dynamic analysis is of added value
  - User emulation matches manual
  - Multiple approaches to emulation

How can malware be tested for detection of antivirus software by emulating user actions, without the AV vendor learning about the malware?

Future work

- Exploratory investigation in traffic generated by AV software
  - Another approach: reverse engineering
- Combine whitelisting with IRMA
- Monitoring AV detection of malware

Questions?