High Performance VM Introspection Using Virtualization Exceptions

Raul TOSA, Senior Manager
Cristi ANICHITEI, Senior Security Researcher

BSides – San Francisco, 2019

Bitdefender

About the Speakers

Raul TOSA

- Senior Manager, Hypervisor and Hypervisor Memory Introspection
- 14 years technical background in malware research, kernel development, hypervisor development
- 11 US patents

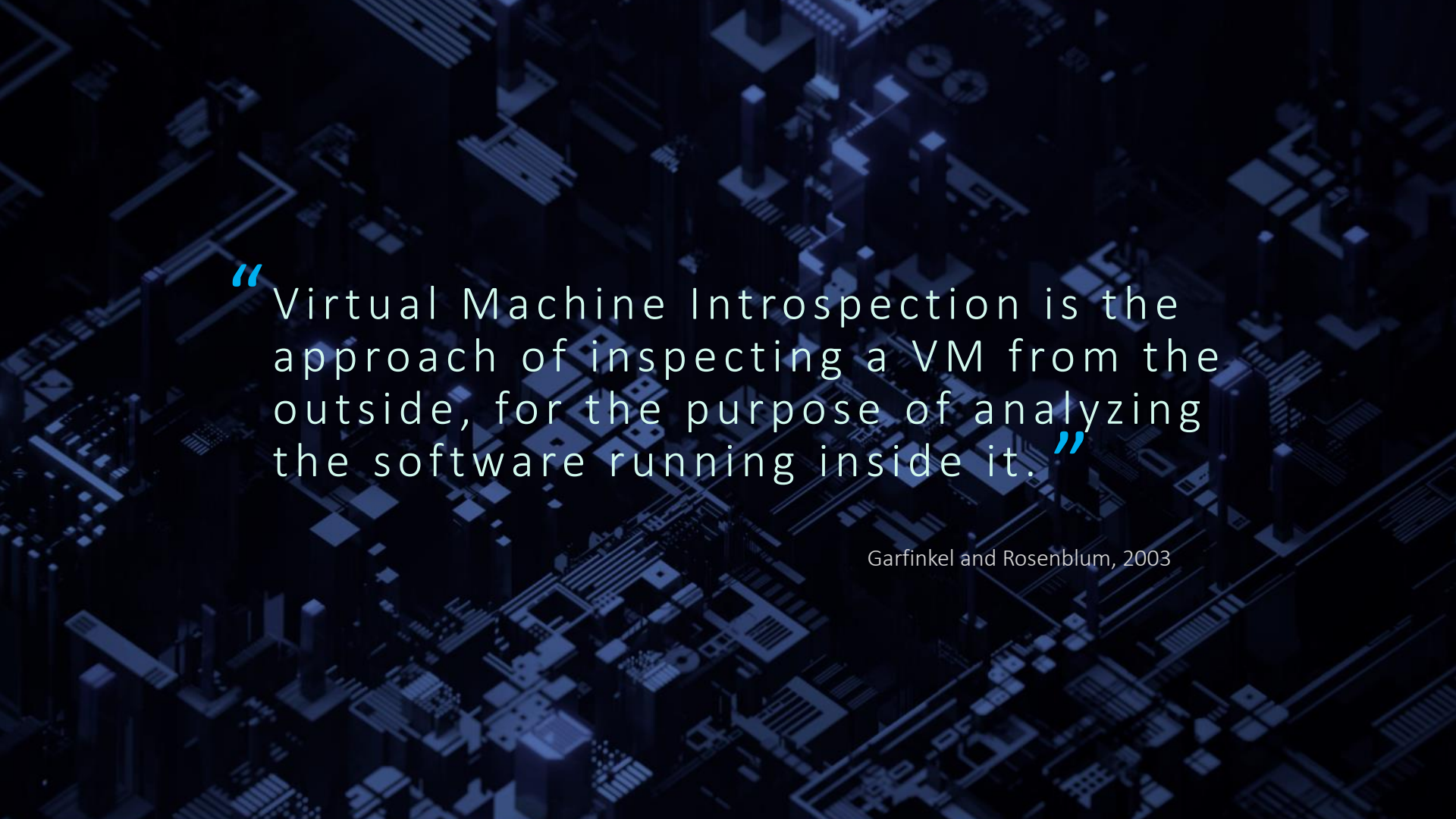
Cristi ANICHITEI

- Senior Security Researcher, Hypervisor Memory Introspection
- HVI development lead (Windows guests); reverse engineering and performance optimizations

Agenda

- Hypervisor Introspection (HVI) in the security landscape
- HVI internals and performance concerns
- Boosting the performance with hardware improvements (#VE)
- Performance figures
- Conclusions

- Q&A: go to https://sli.do from your mobile device to submit your questions (event code: #BSidesSF2019)


“Virtual Machine Introspection is the approach of inspecting a VM from the outside, for the purpose of analyzing the software running inside it.”
Garfinkel and Rosenblum, 2003

APT Lifecycle

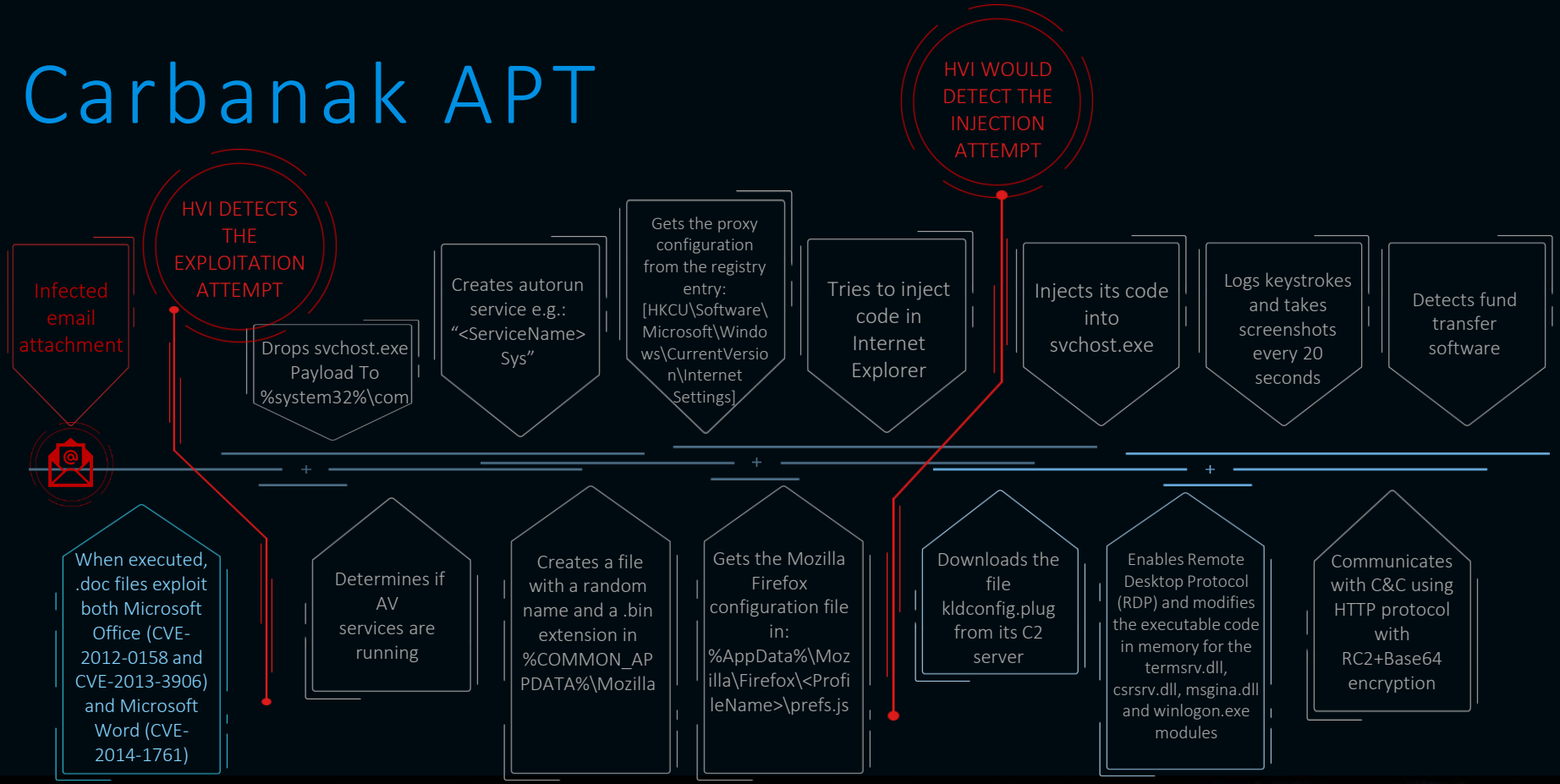
APT Dwell Time

The global median dwell time is reported to be 101 days*

- Americas: 75 days
- APAC: 489 days
- EMEA: 175 days

- M-Trends Report, 2018
- * https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

Carbanak APT



Turla APT

Infected email attachment

Exploitation attempt (CVE-2013-3346, CVE-2013-5065, etc)

Exploit tries to install the kernel-mode driver

The dropper also extracts the user-mode DLL, which is injected into some of the system processes and

The backdoor sends a pack with the victim's system information to the C&C (encrypted)

Other tools (e.g. "winrs.exe") are often uploaded by the attackers to the victim's machine

HVI DETECTS THE EXPLOITATION ATTEMPT

HVI WOULD ALSO DETECT THE ROOTKIT ACTIVITY

Sets itself as a service via registry key HKEY_LOCAL_MACHINESystemCurrentControlSetServicesUltra3 and sets several mutexes to avoid repetitive infection by the dropper.

Connect to a C&C server

Attackers upload a keylogger saved as "C:\Documents and Settings\All users\Start Menu\Programs\Startup\winsvclg.exe"

WildNeutron APT

Leverages an unknown Flash Player exploit

HVI DETECTS UNKNOWN EXPLOITS

Tries to load a kernel rootkit that would hook the kernel and netio.sys

HVI WOULD DETECT THE ROOTKIT ACTIVITY

Dropper is securely deleted by overwriting its content with random numbers several times before renaming and removing the file

Attackers use a range of different tools to extract sensitive data and control the victim's machine (e.g. password harvesting trojan, a reverse-shell backdoor and customized implementations of OpenSSH, WMIC and SM)

Downloads dropper in one of the following locations: "%APPDATA%\Roaming\", "%ProgramData%\Realtek\", "%APPDATA%\Roaming\", etc.

Dropper signed with a stolen, yet valid Acer Incorporated certificate

Drops a Jripbot backdoor as "IgfxUpt.exe" and configures it to use a C&C

Backdoor establishes C&C communication

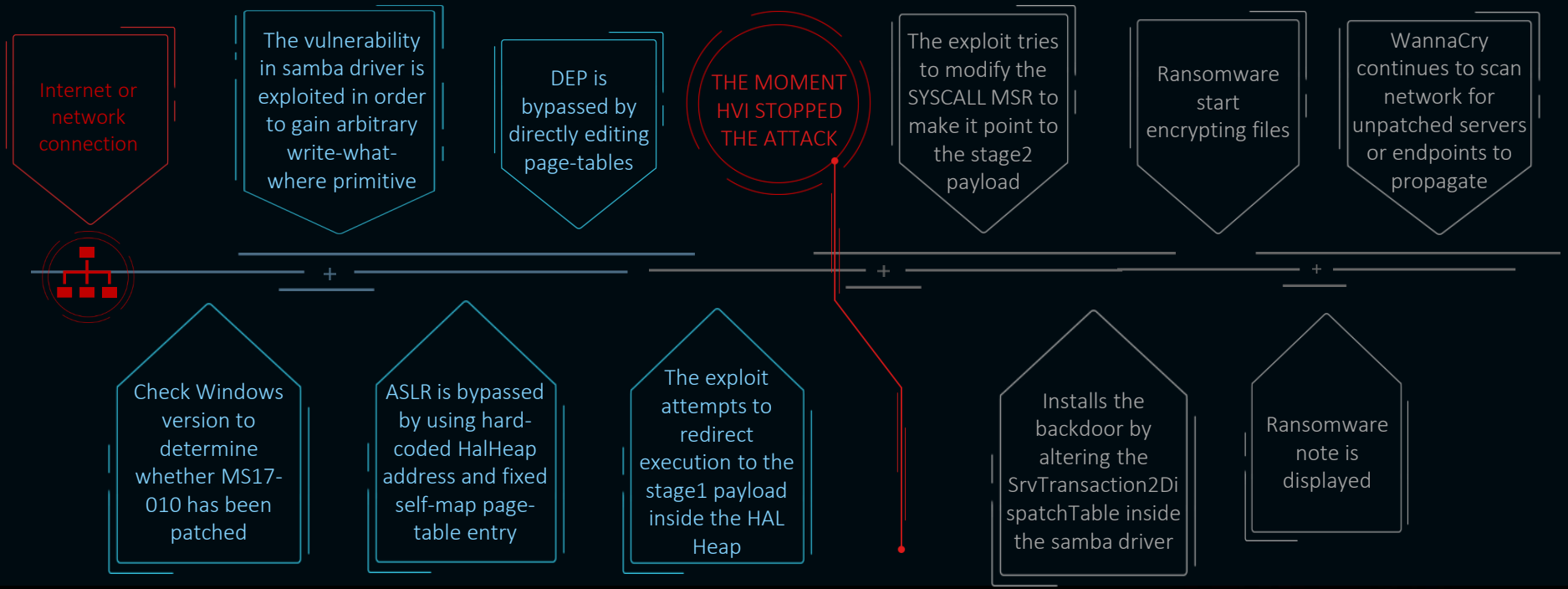
Lateral movement

EternalBlue Exploit

- Supposedly developed by NSA
- Leaked in April 2017 by ShadowBrokers
- Used in May 2017 by WannaCry attack (150 countries, $4B losses*)
- Later used in NotPetya attack (June 2017), Retefe banking trojan (September 2017) and others
- No Bitdefender Hypervisor Introspection customers affected by any of these attacks

* https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

EternalBlue and WannaCry

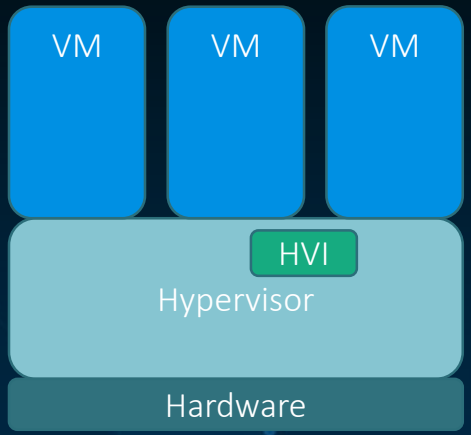


Hypervisor Introspection

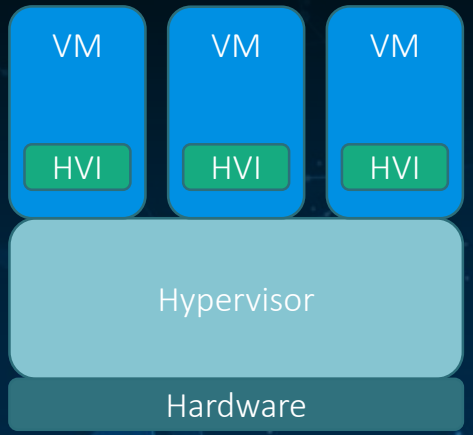
HVI Crash Course

- Runs **outside** the protected operating system
- **Bridges** the semantic gap
- Leverages virtualization features in order to provide protection
- Protects both the **kernel** and **user** space

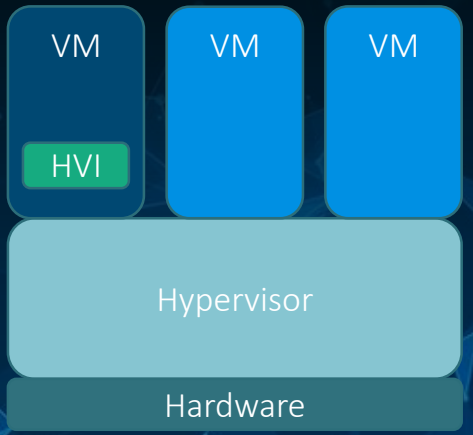
HVI Deployment Models



HVI alongside the hypervisor

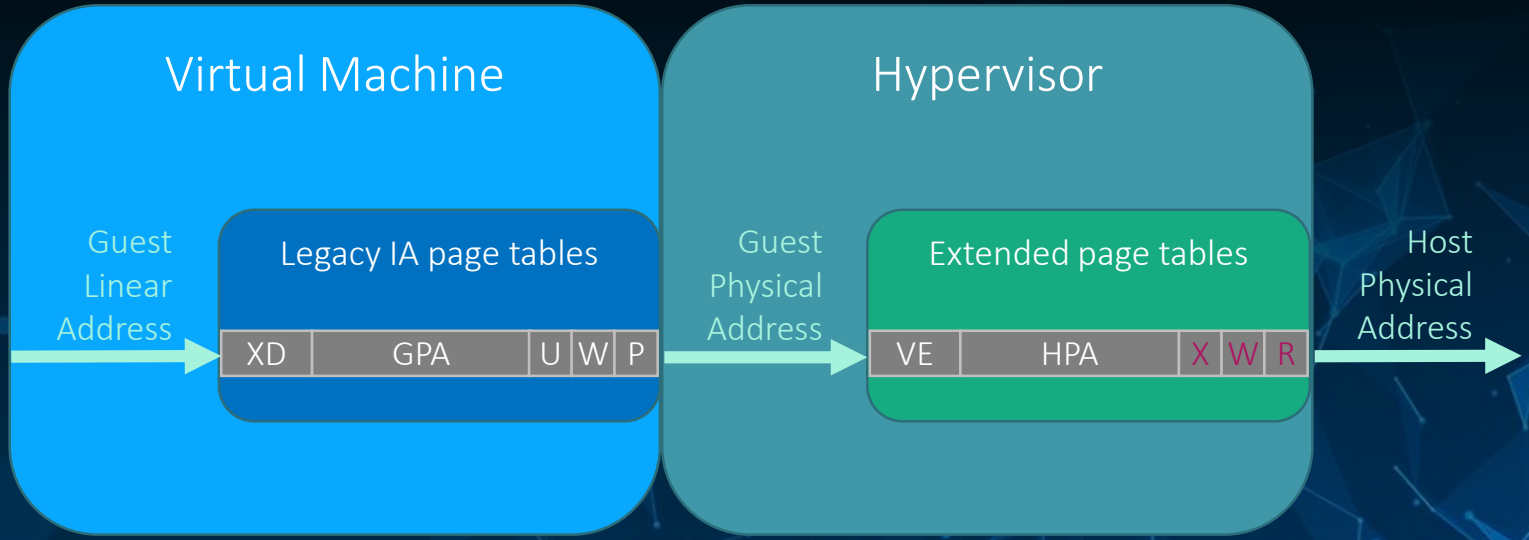


HVI inside each VM



HVI inside a dedicated VM

Protecting the Memory



Protecting the Memory

- Preventing **writes** inside critical structures, such as driver objects, module code and read-only sections, IDT, GDT, etc.
- Preventing instruction **fetches** from memory area that are not executable, such as stacks or heaps

Protecting the Memory

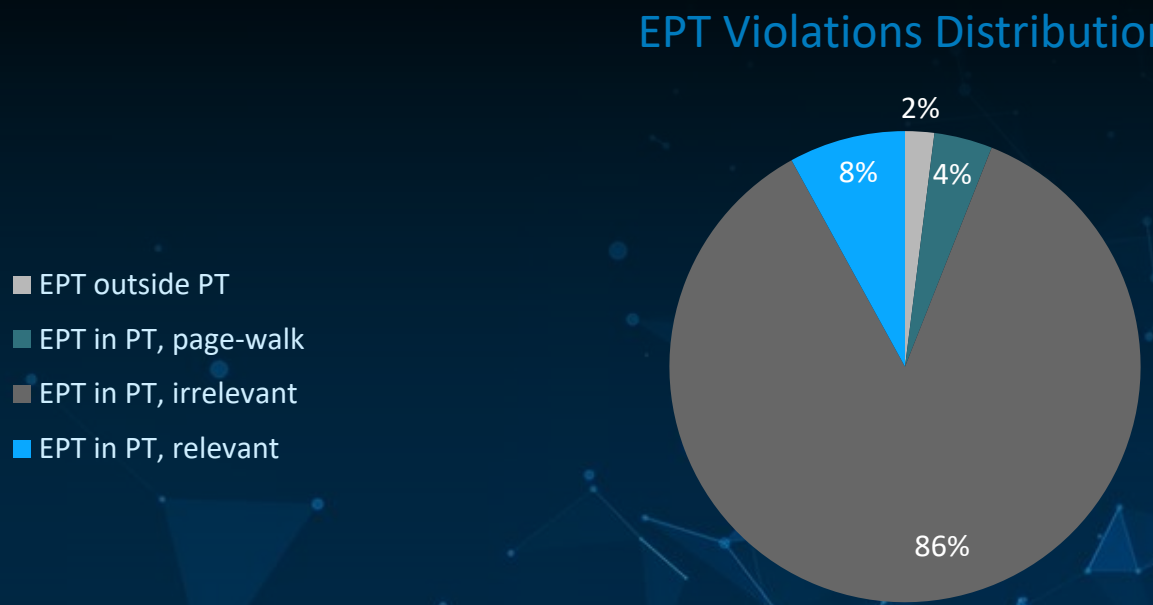
- Problem: HVI protects **guest physical pages**, but the OS uses **guest linear addresses** which may change translations or be swapped in and out
- Solution: HVI intercepts accesses to all levels of in-guest legacy page tables in order to maintain proper protection for guest linear pages

Performance Concerns

Main Performance Limitations

- Most EPT violations are inside page tables
- Most page tables modifications are not relevant

Main Performance Limitations



Boosting Performance With #VE

Improving Page-Table Monitoring

- Use **#VE** to convert EPT violations to an exception that will be delivered to the guest
- Inject a filtering stub inside the guest
- Protect the stub by isolating it inside a dedicated physical address space
- Switch between different EPTs without triggering a **VMEXIT** by using the **VMFUNC** instruction

Improving Page-Table Monitoring

- A preinstalled filtering agent is vulnerable to attacks
- A dynamically injected stub is more secure

Improving Page-Table Monitoring

- HVI creates a new EPT view for the filtering stub
- HVI configures #VE and VMFUNC
- The filtering stub intercepts the #VE handler on each CPU
- The filtering stub handles #VE events: discard un-needed events, report relevant ones to HVI

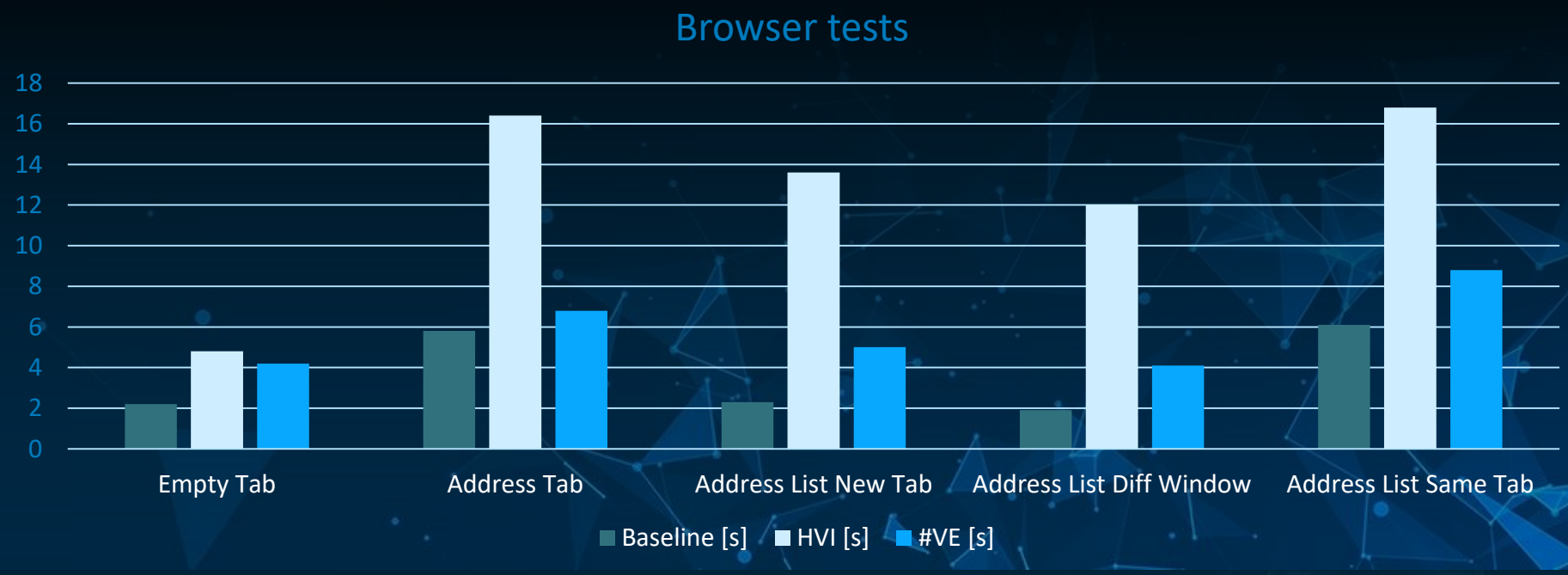
Improving Page-Table Monitoring

- Isolate the filtering stub using a new, trusted, EPT view
- The normal EPT is considered untrusted
- The stub is read-only in the untrusted EPT and as RWX in the trusted EPT
- The OS is RWX in the untrusted EPT and RW- in the trusted EPT view
- Trampoline page used to switch between EPTs is executable in both views

Improving Page-Table Monitoring

- PT access made by the CPU page-walker: emulate
- PT access that modifies unmonitored PT entries: emulate
- PT access that does not change relevant bits: emulate
- Everything else: notify HVI

Performance Figures



Conclusions

Takeaways

- Security doesn’t just “happen”
- You can leverage your hypervisor to keep you safe
- Memory introspection – as approach – has proven effective against most dangerous APTs
- Latest VT-x improvements allow much better performance

Q&A

Submit your questions at https://sli.do (event code #BSidesSF2019)

Meet us at RSAC Booth #2051


Bitdefender®
www.bitdefender.com
Meet us at RSAC Booth #2051