Lies, and Damn Lies:

Getting Past the Hype of Endpoint Security Solutions

Disclaimer

The testing methodology and techniques used during this presentation are not meant to discredit any endpoint protection solution.

All results represent a point in time and results may differ based on different malware sets and different testing strategies. Solutions used between Dec 2016 – May 2017 were current, up to date and configured by each vendor. Some products may have changed or may have been revised since testing was last performed.

This presentation serves only to give back to you, our peers and provide you with a testing framework to help you to effectivity conduct EPP testing on your own. We are not sharing this information for financial gain!

Our opinions are our own and not that of our employers.

Thanks to the Consumer Review Fairness Act of 2016 contracts that purport to restrict our ability to publish these reviews, are void.

Who we are

Lidia Giuliano @pink_tangent

- Information Security Professional for the past 15 years
- In my spare time I research new technologies, build and break stuff

Mike Spaulding @fatherofmaddog

- Information Security Professional for the past 20 years
- I work too much, don't drink enough but love what I do

Agenda

- Our Story
- Endpoint Summary – Lies and Truths
- How to Prepare
- Pre-Execution Testing
- Detonation Testing
- Targeted Attacks
- Summary
- Sound Bytes

Plus
DEMOs

Our Story

Task: To resolve the issue of rampant ransomware, specifically impacting network shares

Challenges faced:

- Clicking on Phishing Campaigns
- Multiple mapping to file shares
- Endpoint User files are encrypted, resulting in encrypted file shares
- Backups and recovery services equated to 2-3 days loss attempting to bring the environment back to 100%

Goal: Dramatically reduce ransomware events (from 10 major to 1 p/yr)

Result: Creation of a framework that went beyond ransomware and using the marketing hype to perform a reusable testing methodology

Lie: Protect Critical Servers

Lie: Protect only your critical servers!

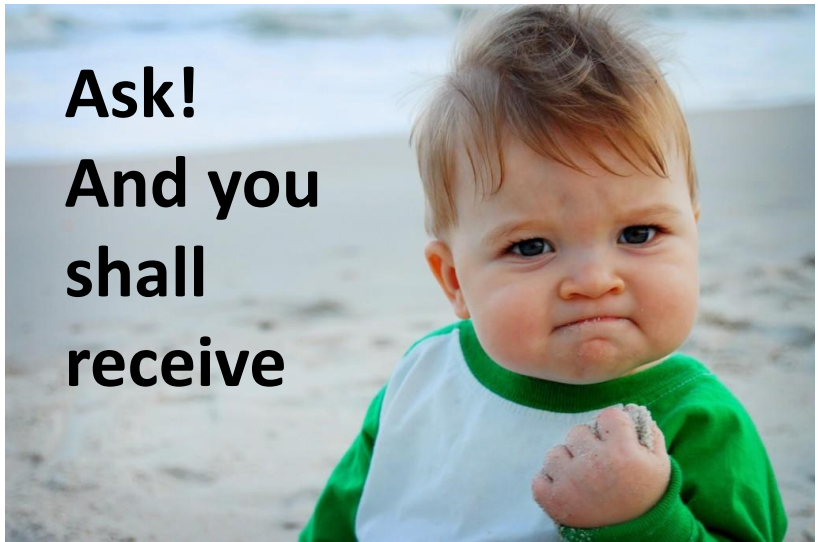
Truth: Deployment is essential!

- File Share protected with an EPP agent
- Patient 0 is not protected or is using traditional AV
- Patient 0 clicks on a malicious attachment and resulting in local files being encrypted on the endpoint
- Will the files on the share drive be spared?????

For consistency, this scenario was tested on across all solutions

Objectives

- Provide an overview of endpoint product (EPP)
- Solutions on the market and knowing where to start
- Company business requirements vs. EPP Solutions
- Planning your POC:
  - Plan / Roadmap
  - Preparation
  - Test Plan
- Provide you with our tools to enable you to test solutions yourself, a testing framework
- **You:** Knowledge!
  - Know the questions to ask
  - Know how to do it yourself



Endpoint Protection Overview

Traditional AV

- Point-in-time
- Signature DAT file
- Blacklists
- Malware is analyzed centrally
- Easy to evade
- Low effectiveness
- Machine degradation due to Pre-execution

Next Gen AV

- Malware analyzed using AI and ML
- Signature-less
- Plus binary detection
- Detection of behavioral patterns
- Cloud for big data analytics
- Zero-day
- Greater rates of effectiveness

Detection and Response

- Detect and respond to IoA
- Incident prevention
- Hunting and Triage
- Visualization & exec details
- File & process (sub) trees
- Network con DNS lookups
- Containment
- IR

Other

- Application Whitelisting
- Remediation capabilities
- Script Control
- Memory Protection
- Firewall
- Sandboxing
- TI Community
- SOC

The Marketing Slogans

Marketing: Real Time APT Protection
Observations: No memory-based analysis

Marketing: Multi-layered Approach
Observations: Turn a layer off, hello malware

Marketing: Leader in Cloud-based Endpoint
Observations: Have a roaming user with no internet connection, product effectiveness drops

Marketing: Complete replacement of your legacy AV
Observations: Do we even have a governing body? There is no regulation. Consider the impact on your compliance needs!

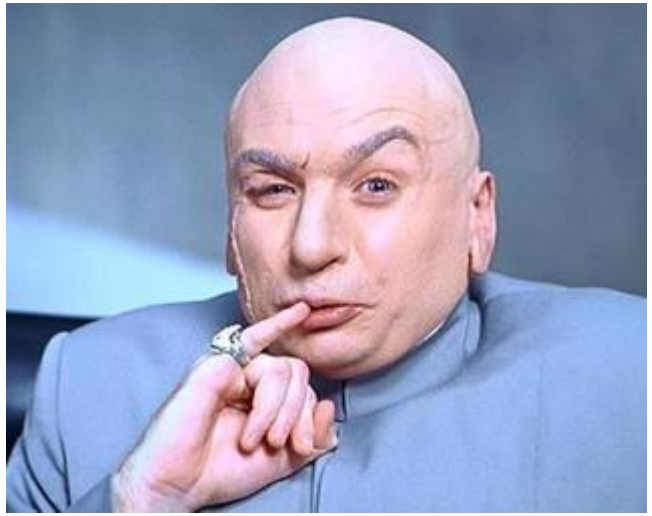
** Not specific to any solution **

Endpoint Protection

What Problem Are You Trying to Solve?

The Problem is not:

- Ransomware
- Insider Threat
- Malicious Outsider
- Data Exfiltration or
- Threat Hunting



Business Centric:

- Reduction of Incidents
- People Costs
- Reputation
- Keep the business running

Backed with metrics, always!

Business Requirements and Values are CRITICAL!

It could be that NONE of these solutions will meet your requirements.

Business Requirements

Oct to Dec 2016

- ~80 functional requirements
- ~20 non-functional requirements
- Five technical testing scenarios each with ten subtasks
- Rinse and repeat for different types of users (admin, developers, standard)
- Different OS
- Cloud on / Cloud off

Testing

Jan to April 2017

- Prepare testing environment
- Collect samples
- Test Pre-Execution
- Test Detonation
- Test All capabilities enabled (best foot forward)
- Static Malware using multiple file types and scripts
- Targeted attacks combination of file and file-less testing specialized

Documentation and Recommendation

April to May 2017

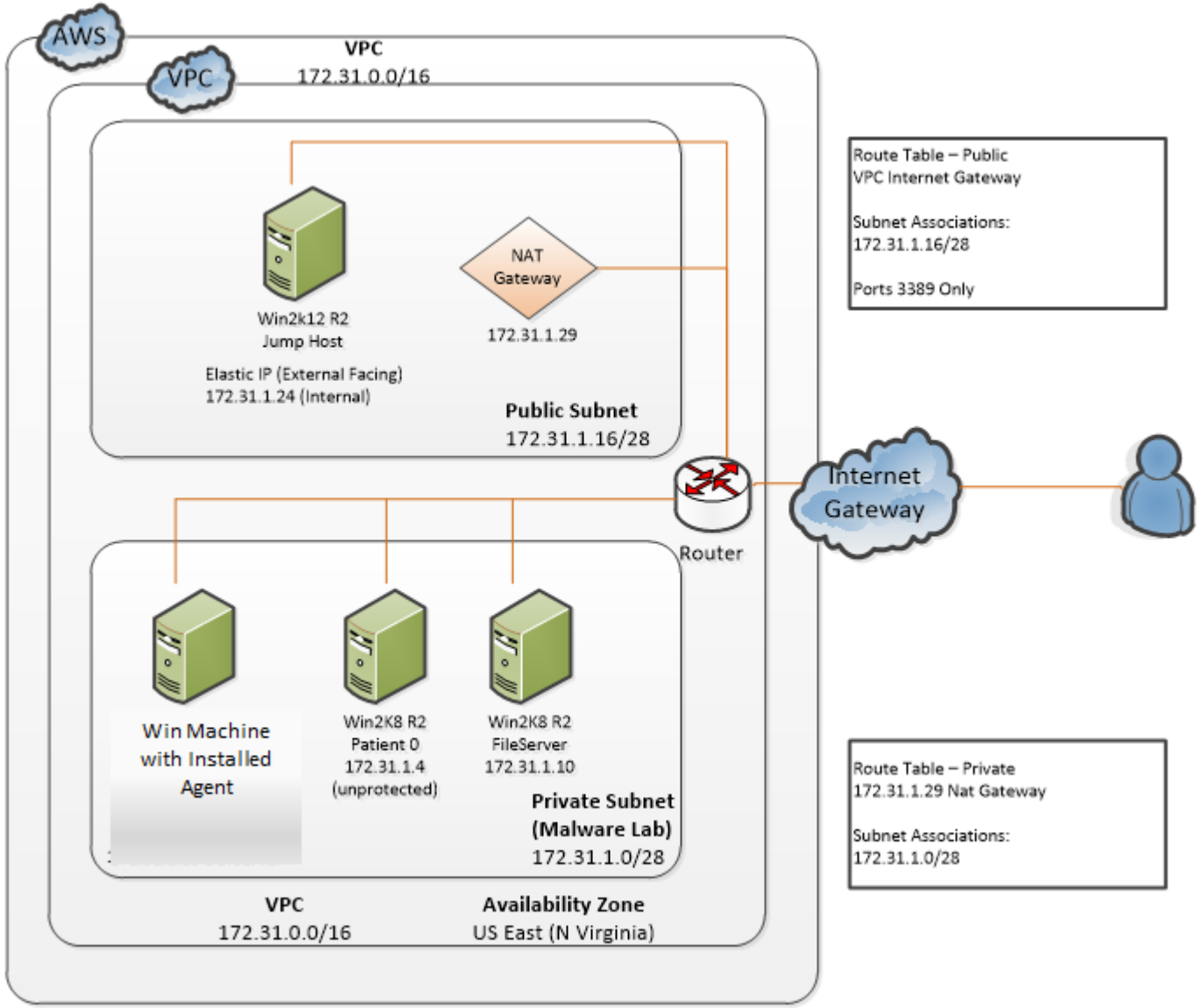
- All statistics gathered and documented
- Executive report generated
- Technical report created
- Recommendation made

Other Business Requirements

Requirements you should consider outside of functional testing:

- Do you want 100% SaaS or hybrid or worth upgrading (RTO)?
- For SaaS, consider your authentication needs, SMS, Auth App, etc
- Do you need AD integration? How many admins will be using it? RBAC?
- Agent installation, will a reboot cause issues?
- Consider **ALL** OS and applications you run. Make sure the agent is compatible, for example, XP with no SPs, Win2K, MacOS, etc.
- Validate the software will run on lower-end machines, for example, 1GB of memory or 1 Core CPU.
- Define your alerting and reporting needs.
- Finally, consider your testing environment! ***Important***!

Preparation – Environment



- All our test machines were fully patched with the EPP agent installed on them.
- Vendor worked with us to create the prevention policies either in their SaaS environment or virtual servers.
- We used their environment to validate and monitor only; no settings were changed.

Preparation – Malware Testing

Where to Source

- **In-house Forensics / InfoSec Teams**
- GitHub Repositories (e.g.: the Zoo)
- Other subscribed services (free / paid)
  Virus Total, Virus Share,
  Malwr, TestMyAv,
  Malshare, MalwareDB, etc

** Important: Have a Variety **

Types (Mix of Old and New)

- Ransomware
- Exploit Kits
- Viruses and Worms
- Backdoors
- Trojans
- Browser Hijack
- RAT
- Bots
- Droppers
- Adware and Spyware

Preparation – Malware Testing

File Types:

- Portable Executables (PEs)
- Other compiled code, vbs, .bin, .com,
- Compressed files, .zip, .jar, 7-zip, etc
- Native windows scripts, batch and ps
- Obfuscate the content in the scripts
- Rename extensions to other file types
- Known Good Files
- Create a FP directory

** Important NOT just binaries **

Mutate the files

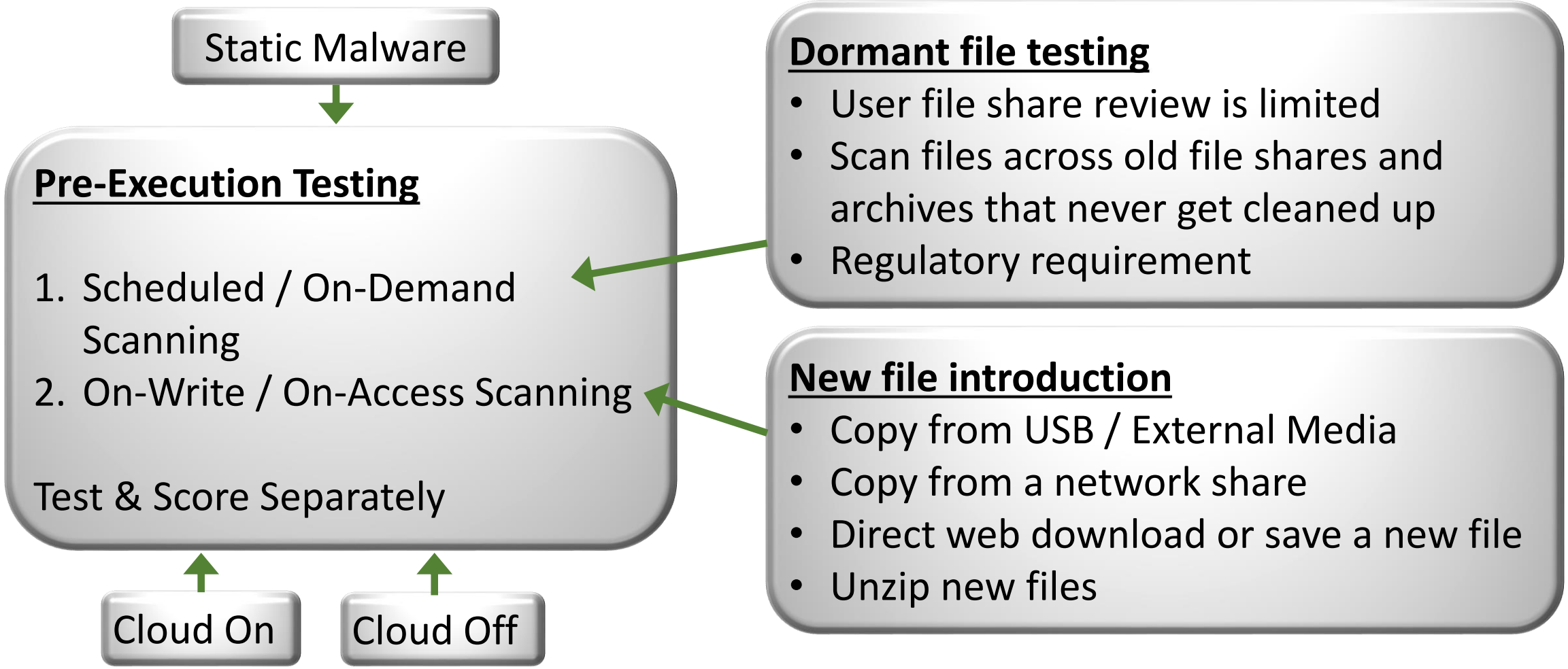
- Packer
- Hash Modifier

(where possible)

Other Important Preparation:

- Testing Platform
- User Privilege

Pre-Execution Testing Approach

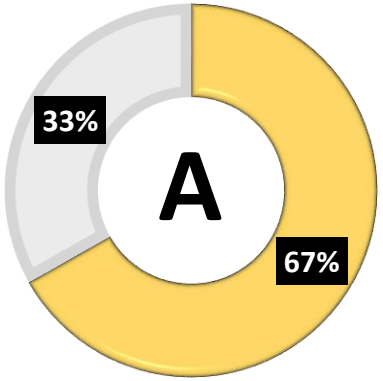


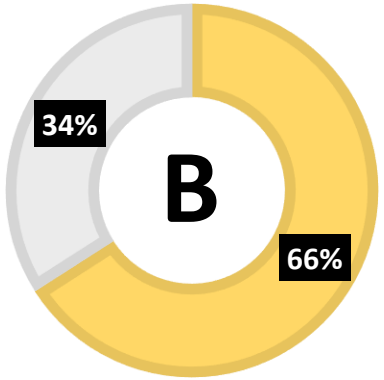
*** During pre-execution, over 40,000 pieces of malware were tested ***

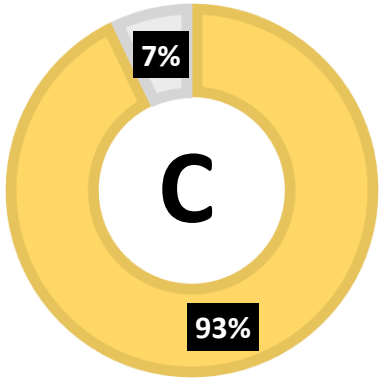
Pre-Execution – Sample Scoring

Sample Pre-Execution Scoring Sheet		Solution 1					Solution 2				
		Scheduled / On-Demand	On-Write				Scheduled / On-Demand	On-Write			
	Total Files	File System	External Drive	Download	Save AS	Copy From	File System	External Drive	Download	Save AS	Copy From
Malware											
Sample Set A - Personal / Company Collection											
Malware Set A	10		7				9	9	9	9	9
Malware Set B	20		15				18	18	18	18	18
Total	30	0	22				27	27	27	27	27
Percentage		0	0.733				0.9	0.9	0.9	0.9	0.9

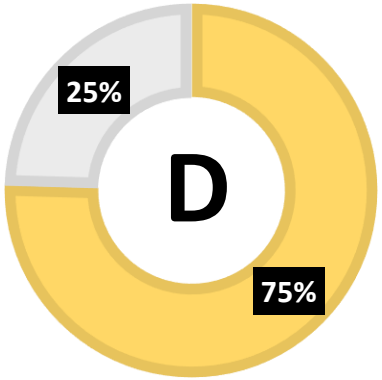
Pre-Execution - Original

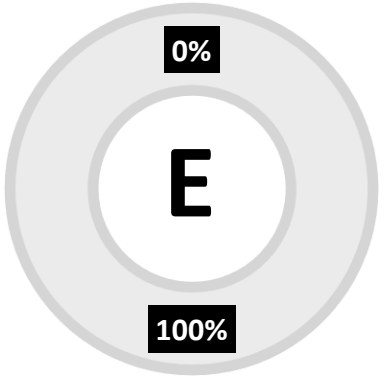






~20,000 samples used

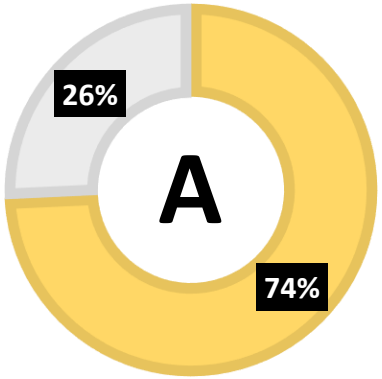


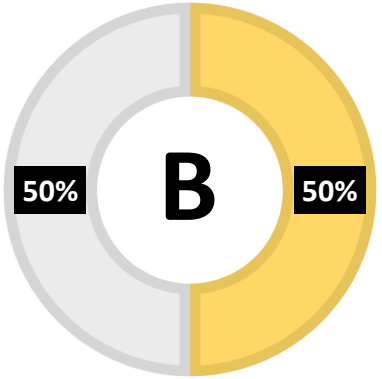


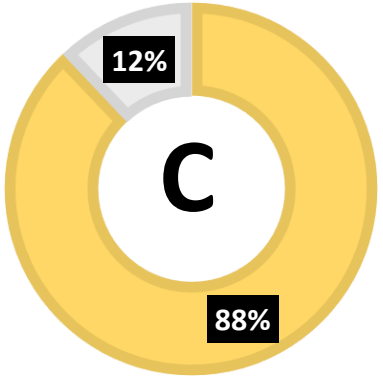
Quarantined

Not Quarantined

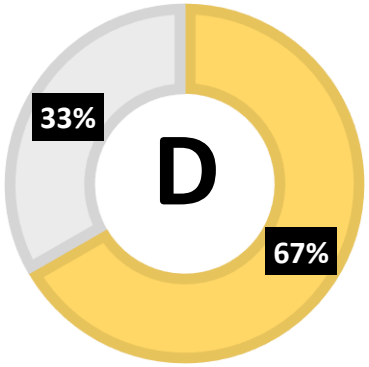
Pre-Execution - Mutated

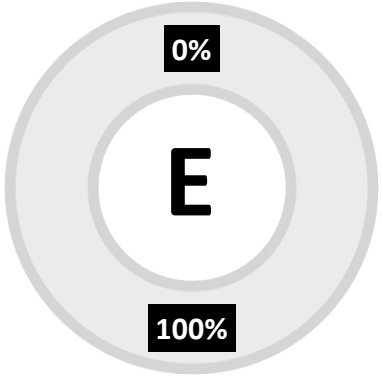






~20,000 samples used

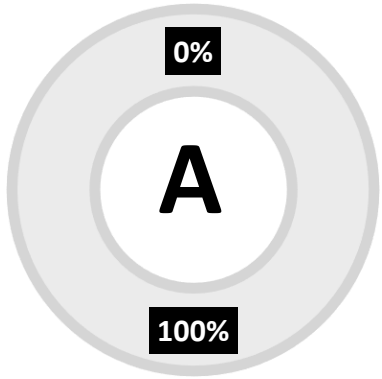


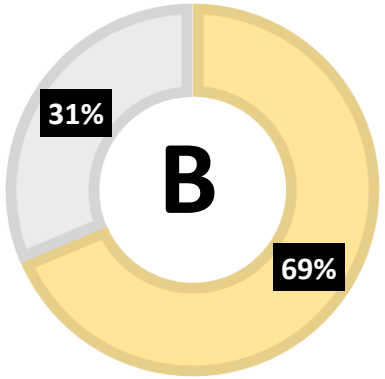


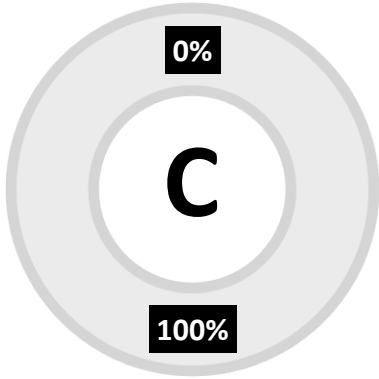
Quarantined

Not Quarantined

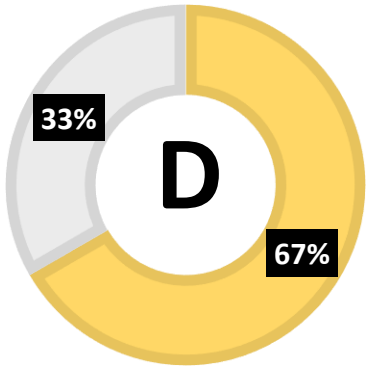
Pre-Execution - Scripts

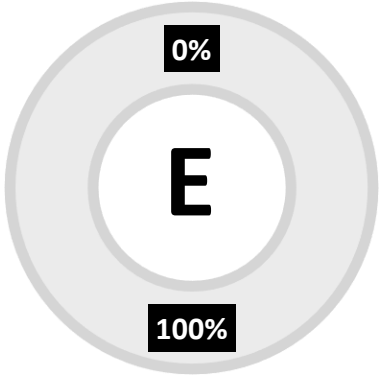






~50 samples used





Quarantined

Not Quarantined

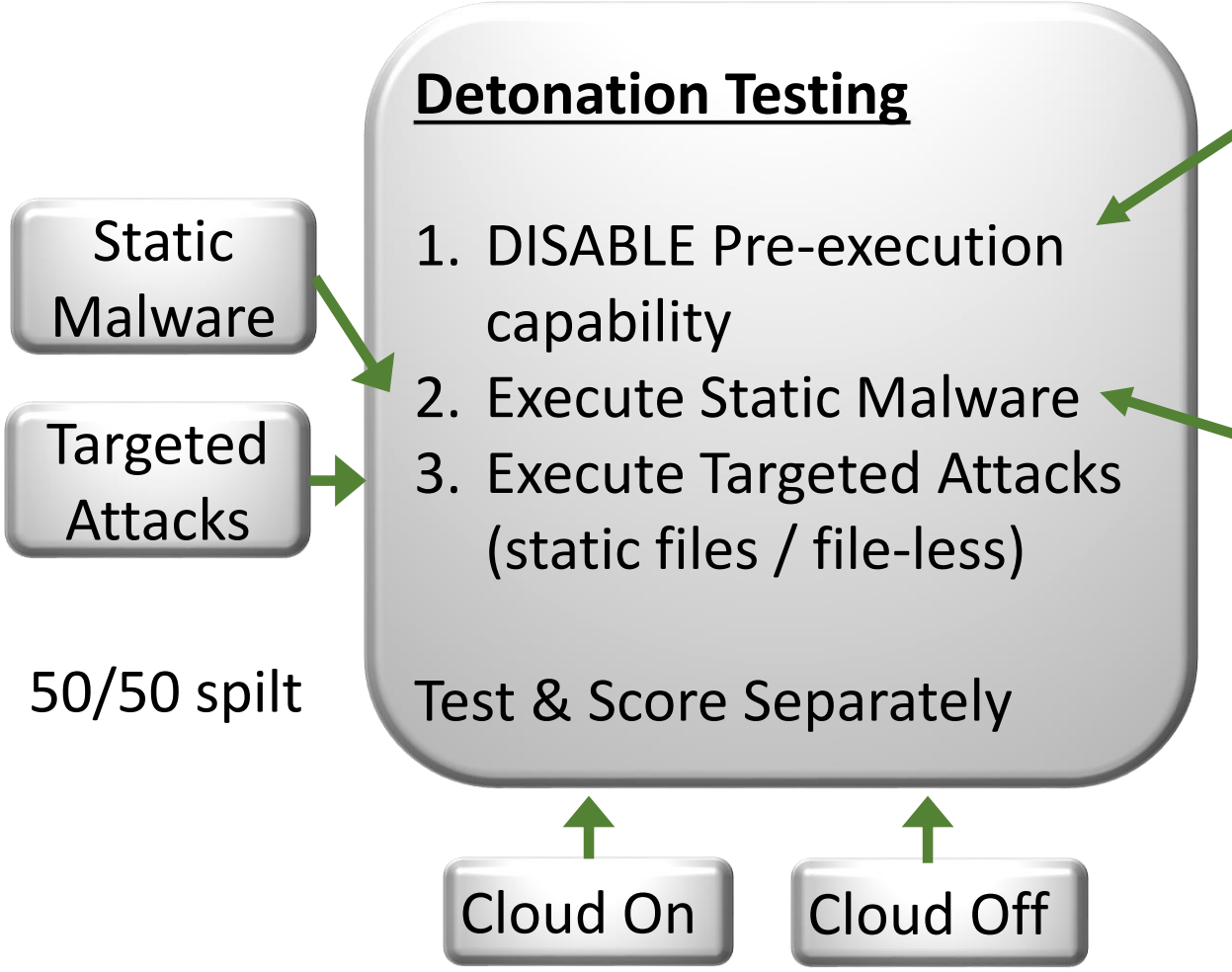
Pre-Execution – Hype Summary

- Some products have on-write and sandbox detonation tightly-coupled. This begs the question, where is the machine learning if you sandbox everything?
- Off Cloud, we observed a reduction in the effectiveness of the results. Was the solution putting all its eggs in the “cloud basket” for testing the malware?
- On Cloud, we noted a delay in killing or quarantining the malware due sandboxing or cloud testing. To what extent is “machine” learning on the agent doing?

Takeaways:

- Marketing that states “COMPLETE AV replacement,” check YOUR requirements. Not all solutions have dormant scan capabilities.
- Is sandboxing productive or a bolt on for dated software that needs to be re-architecting?

Detonation Testing Approach



Disabling pre-execution controls enables you to measure the coupling between solution modules and its ability to detect/prevent if something fails or evasion strategy

Static Malware

Using the malware from the pre-execution phase, detonate using different techniques

- standard command line detonation
- batch script
- PowerShell script
- anything native to windows or specific to your environment

Detonation – Sample Scoring

Sample Detonation Testing Only
Scoring Sheet

Method A: Good for Large Volumes
Method B: Good for Specific Tests or Attack Vectors (EDR-type solutions)

		Method A			Method B			
	Total Files	Quarantined	Process Stopped Not Quarantined	Process Executed	Quarantined	Process Stopped Not Quarantined	Process Executed (Detected)	Process Executed (Not Detected)
Malware								
Malware Set A - Company Samples								
Set A	10	9	1	0				
Set B	5	4	0	1				
Total	15	13	1	1				
Malware Set B - xx								
Set A								
Set B								
Total	0	0	0	0	0	0	0	0

Detonation (Pre-Exec Off)

Detonation of Malware Demo

Scenario:

- Pre-execution engine disabled
- 100 pieces of malware executed sequentially using a **batch** script

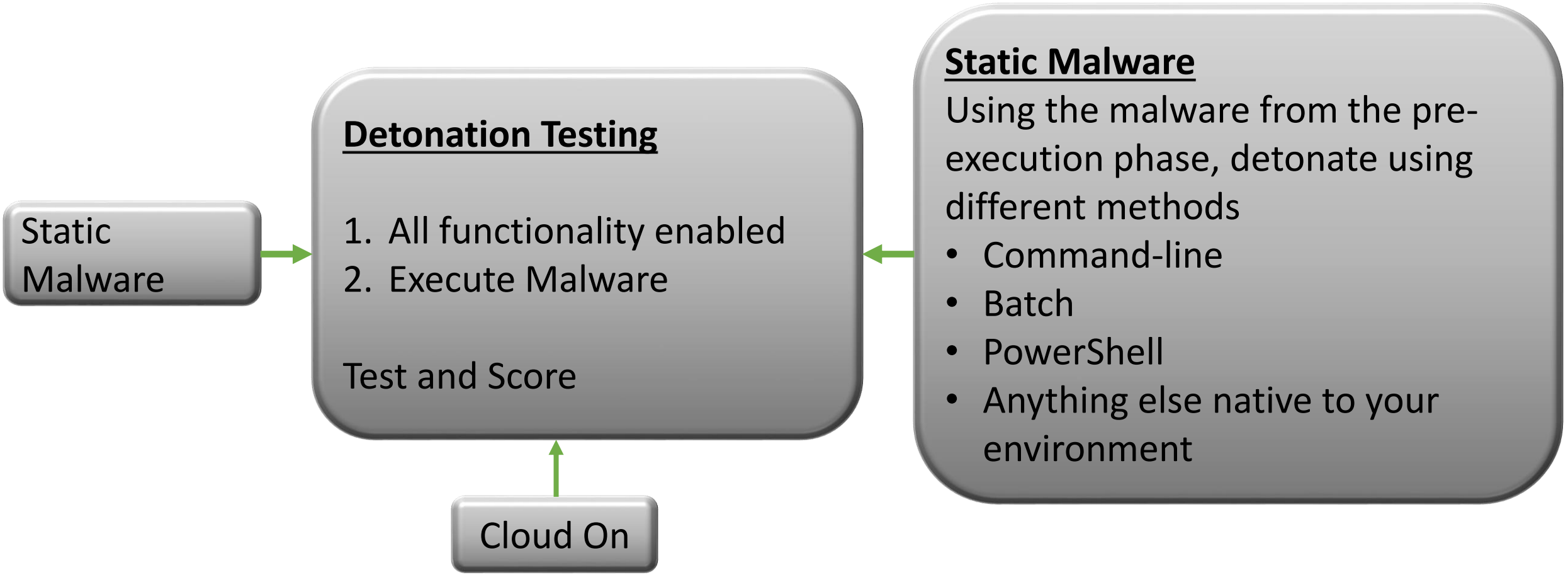
Detonation (Pre-Exec Off)

Detonation of Malware Demo

Scenario:

- Pre-execution engine disabled
- 100 pieces of malware executed sequentially using a **PowerShell** script

All Capabilities Enabled Testing



Detonation – Sample Scoring

Sample All Capabilities Enabled Scoring Sheet

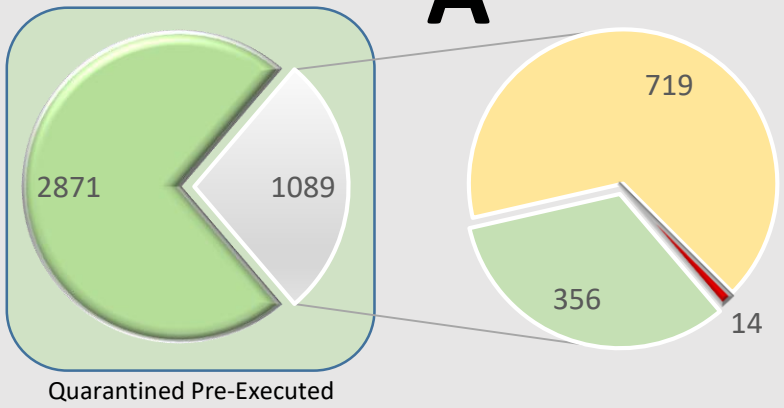
Method A: Good for Large Volumes

Method B: Good for Specific Tests or Attack Vectors (EDR-type solutions)

		Method A						Method B					
		Pre-Exe		Execution				Pre-Exe		Execution			
Malware Samples	File Count	Pre-Execution Quarantined	Pre-Execution Files Remaining (After)	Quarantined	Process Stopped Not Quarantined	Process Executed		Pre-Execution Quarantined	Pre-Execution Files Remaining (After)	Quarantined	Process Stopped Not Quarantined	Process Executed (Detected)	Process Executed (Not Detected)
Malware Set A													
Sample A	5	3	2	1	1	0							
Sample B	4	4	0										

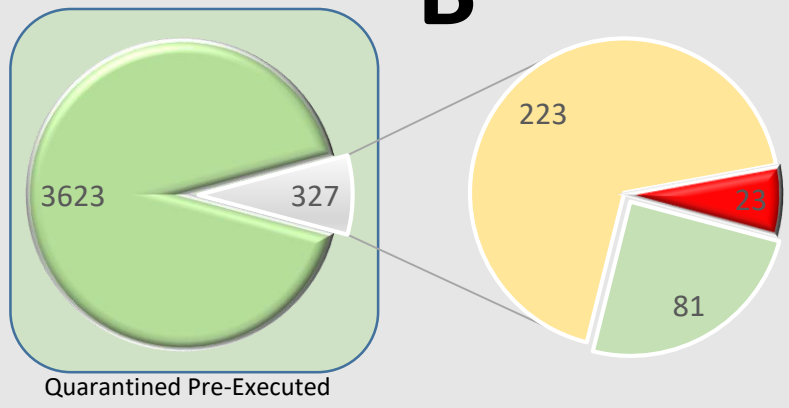
All Capabilities – Known Malware

A



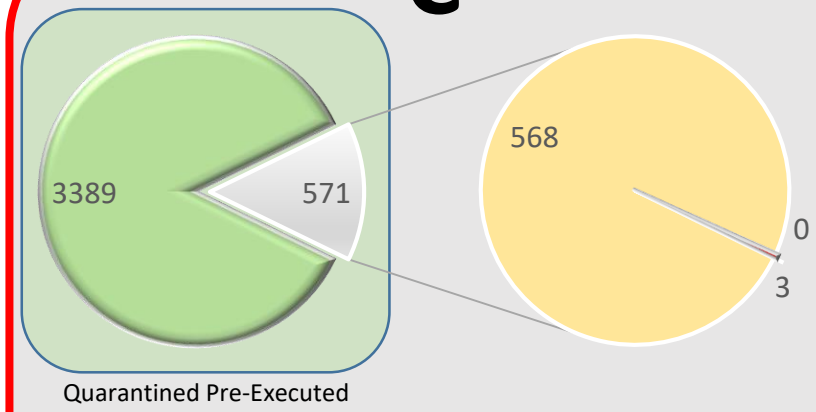
Of the malware which infected this EPP, re-tested 3 times over a period of 3 weeks. There appeared to be no machine learning or behavioral changes.

B



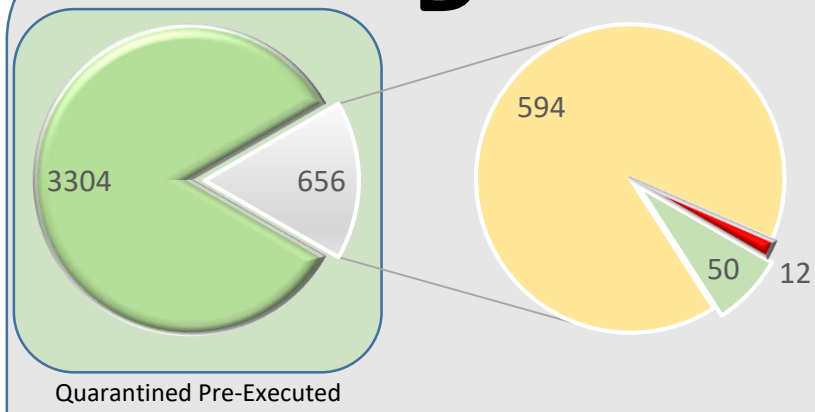
Of the Malware executed this caused the machine to be shutdown 3 times.
No learning or behavioral changes after re-testing.

C



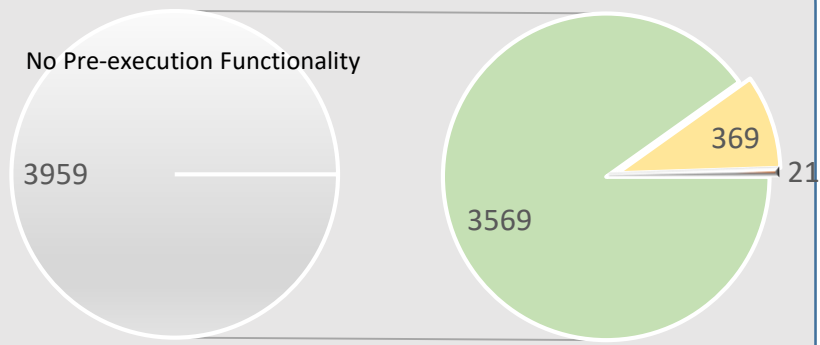
Only a few PUP software executed

D



Only a dozen PUPs executed

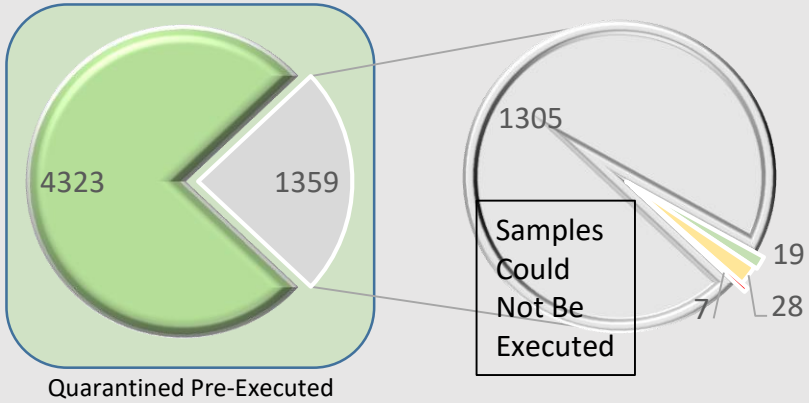
E



Of the malware executed during the first pass, none were executed during re-testing

All Capabilities – Mutated Malware

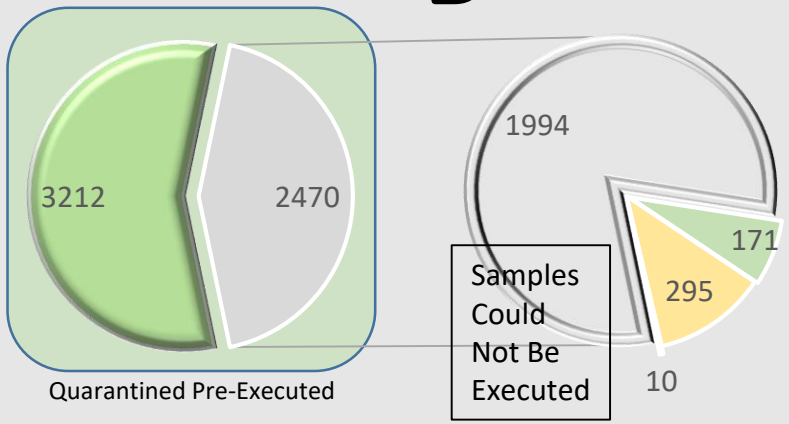
A



Re-testing showed no difference in results.

Not all files tested due to the system being white screened or shutdown.

B

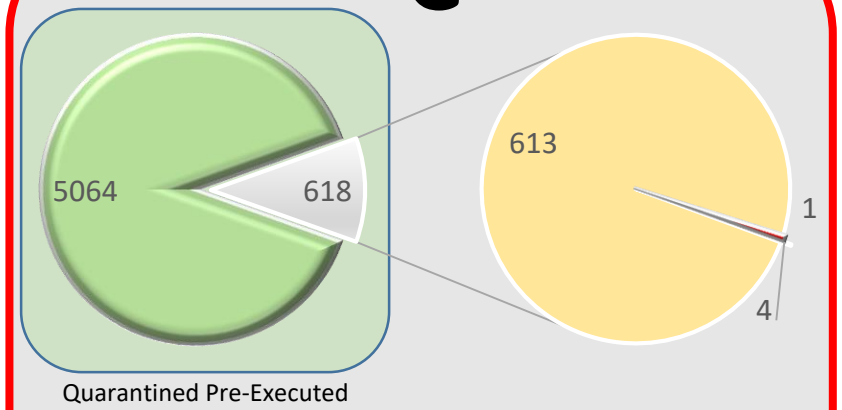


Very slow executing mutated samples.

Remaining malware caused the machine to shutdown 4-5 times.

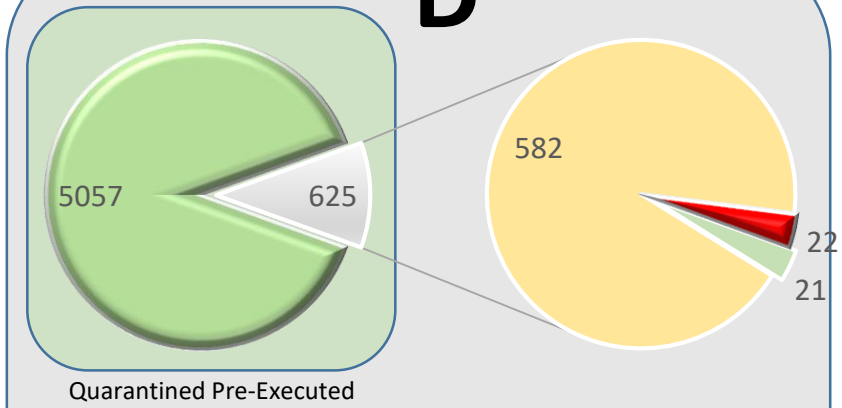
No change when re-testing.

C



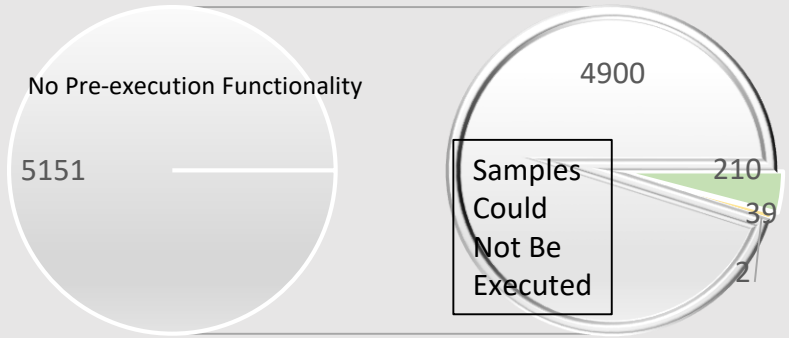
Agent quarantined or stopped almost all mutated samples.

D



Slow execution of mutated samples. Agent protected against most of the malware with machine shutdown 1-2 times.

E



Of the mutated sets, this agent machine learning ability was strong. However, the last sample set caused multiple machine shutdown.

All Capabilities

All Capabilities Enabled Demo

Scenario:

- 100 pieces of malware executed sequentially using a via **the command line**
- 100 pieces of malware were mutated two times using two different methods to change their hash values
- Machine is “double-ransomwared”

Detonation – Hype Summary

- Detonate your malware using different methods, not just click and execute
- Mutate your malware using different methods for a zero day effect
- Sandboxing technologies took hours to test large amounts of malware compared to minutes of the NextGen solutions.
- Re-testing mutated malware resulted in little to no changes
- Takeaways:
  - How effective is sandboxing on off network users
  - Consider the impact to system resources when using a sandbox
  - Tight coupling of solution capabilities could reduce your capture rates
  - How much is RT machine learning vs. machine learning to reactivity create more signatures? Or IoC vs. IoA?

Targeted Attack Testing

Attack Testing

1. Attacker machine (Like Kali)
2. Victim (Win 7, 10)

Test and Score

Spilt 50/50

Scenario

- Simulate Phishing Attacks
- Browser Exploits
- Reserve Shell
- Endpoint Recon
- Windows Exploits
- Credential Dumping
- Lateral Movement
- Gaining Persistence

Advanced Testing
May require extra resources

Target Attack Testing

Batch and Powershell Testing

- Malware Obfuscation
- Using PS to execute other processes
- Obfuscation of script variables
- Base64 Encoding
- Use what is available natively on your SOE build

Social Engineering Attacks

- Attachments
  - Binary Files
  - Macros
  - PDFs
  - Scripts
- Weblinks
  - Internet Explorer Exploits
  - Window Exploits
  - Java Exploits
  - Gaining Reserve Shell & Doing simple recon

** Scoring: Can use detonation spreadsheet **

Target Attacks

Target Attack Demo

Scenario:

- Using Kali (attacker), exploit MS11-003 used against victim running an unpatched version of IE
- Victim gets link and clicks
- Attacker takes advantage of vulnerable IE and obtain a reserved shell on the victim's machine
- Attacker start recon

Target Attack – Hype Summary

- Most solutions performed well in this category blocking phishing attempts, either by attachment or browser exploit which tried to run memory-based malware

Takeaways:

- EDR solutions are great for threat hunting teams, given the visualization and depth of data, but are you company ready!? Can you handle the truth??
- If you can reverse shell in, some solutions may not see this as an IoA, not until you do something suspicious
- TI simply does not work! With many content filtering solutions unable to categorize malicious domains rapidly, how is the TI used by these solutions any different? What are they doing differently?
- Ultimately, a well-funded, motivated adversary will manage to compromise your security. It is important to understand the vision and direction of the vendor to understand how their R&D will drive them toward improving their solution.

Decision Analysis

Must(s)	Vendor A Comments	Y/N
Pre-execution scanning of dormant files		Y
Pre-execution of file on-write		Y
Pre-execution Capture 80%+ (includes PE and Scripts)	87.67% - no script scanning	Y
Malware Detection		Y
Preventation Rates 95%+ (all types of families) - orginal	99.47%	Y
Preventation Rates 95%+ (all types of families) - mutated	99.35%	Y
Can run in parallel with XYZ?	Complimentary to XYZ AV	Y

Want(s)	Weight	Comments	Score	Total
Functional Testing		Functional Testing		
Managed from a Cloud-Based Solution	10	SaaS MGMT & Patching from Cloud	10	100
Threat Intelligence: Data Sharing	10	Outside Sources	10	100
Log Management: Verbose Logging	8	Log API - Extensive Logging	10	80
Section Weight	20%	Section Total		280
		Weighted Section Total		56
Non-Functional Testing		Non-Functional Testing		
Installation Process	10	Light Package, Quick Install	10	100
Vendor Support	10	Quick Response	10	100
Reporting Services	10	Module is a work in-progress.	6	60

Section Weight	20%	Section Sub-total	260
		Section Weighted Total	56
Machine Learning/Behavior Detection		Machine Learning/Behavior Detection	
Ability to detect known malware (Morphed)	10	ML was best of all,	10 100
Ability to detect older mutated vulnerabilities	10	Had nearly a perfect rate of detection of mutated samples	10 100
Updates to the Code (Timely)	10	Monthly Update	8 80
Section Weight	20%	Section Total	200
		Weighted Section Total	40
Performance & Scalability		Performance & Scalability	
Ability to withstand a large scale attack	10	Quarantined 5000/5000	10 100
Size & Speed of Agent	10	Light Agent (No Signatures)	10 100
Compatibility with Operating Systems	8	No additional upgrades needed	10 80
Section Weight	20%	Section Total	280
		Weighted Section Total	56
Financial Expenses		Financial Expenses	
Units/ Annum			5 0
Section Weight	20%	Finanical Rank	1
		Weighted Section Total	60
		Weighted TOTAL Score	268

Summary

- All these solutions had great offerings and will provide much better protection than signature-based solutions
- There is NO SILVER bullet, and an advanced adversary will find a way
- These solutions serve as an extra control; there is no substitute for defense in depth
- Before you decide to go down this path, evaluate if there is anything extra you can do from an infrastructure perspective to add more defensive layers and minimize lateral movement of malware.
- Ask yourself are you using all the current capabilities you have today to their fullest potential?

BlackHat Sound Bytes

- Test for yourself!
- No silver bullet – Use all the capabilities you have
- There is no substitute for Defense in Depth

Thankyou

Special Thanks To:

- EFF for their great legal advice
- Our forensic team for providing company samples
- Our vendors who seriously were awesome folks who provided exceptional service and fast response to our many many questions
- Our families for their love and support during the months of preparation leading up to BlackHat

Questions

Contact Information:

Lidia Giuliano on Linkedin
Twitter: @pink_tangent or
Email: tangentmelb@gmail.com

Mike Spaulding on Linkedin
Twitter: @fatherofmaddog or

References

- SANS Institute:
  - Out with the Old, In with the New: Replacing Traditional Antivirus
- Gartner Papers:
  - Magic Quadrant for Endpoint Protection Platforms
  - Comparing Endpoint Technologies for Malware Protection
  - Comparison of Endpoint Detection and Response Technologies and Solutions
  - Market Guide for Endpoint Detection and Response
- Mitre ATT&CK Adversarial Tactics, Techniques and Common Knowledge https://attack.mitre.org/wiki/Technique_Matrix
- Various: Vendor solution testing guides
- Various: Webinars, Blog Posts, Podcasts
- Github for Malware Samples and other subscription services
- Testing guides found on AMTSO, TestMyAV, other countless research papers