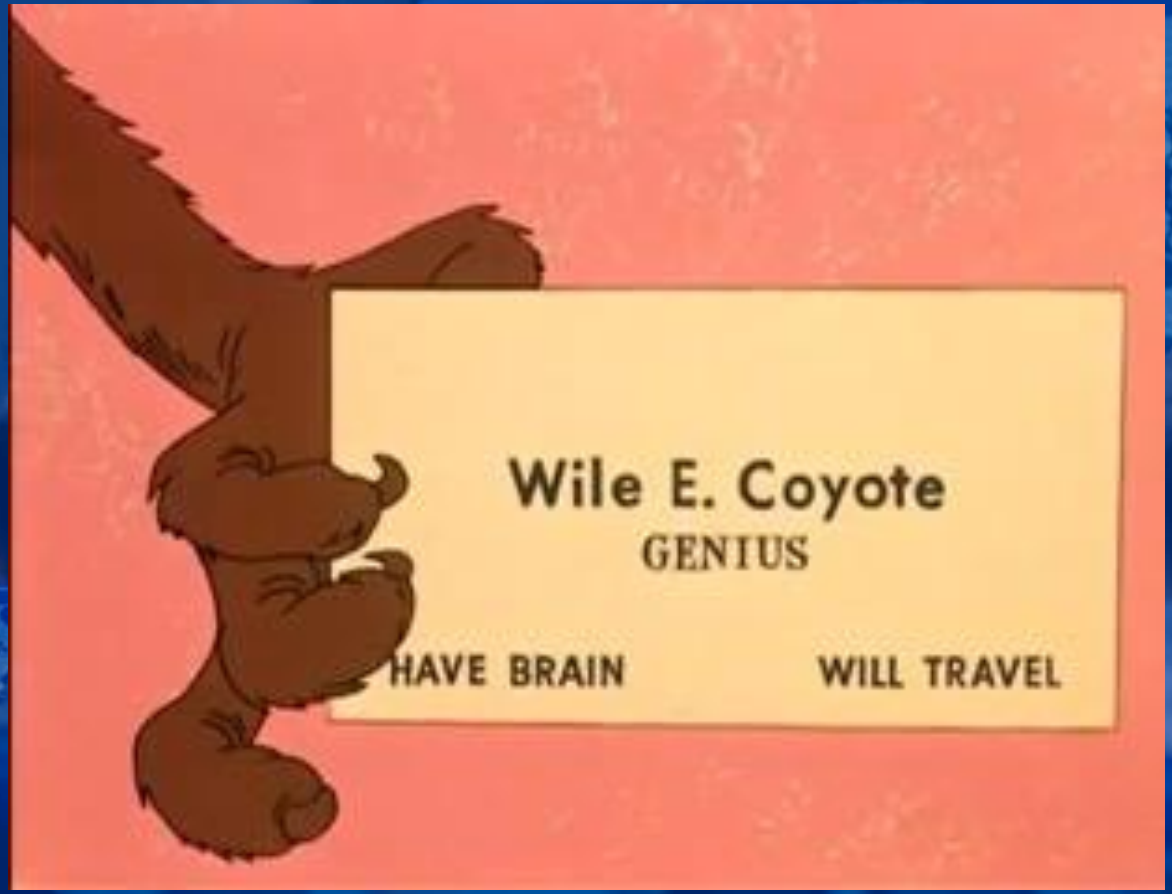
The Cybersecurity Threat Landscape

Vikram Phatak, Founder at NSS Labs

NetEvents Global IT Summit

October 3, 2019


Wile E. Coyote
GENIUS
HAVE BRAIN
WILL TRAVEL

Global Cost of Cybercrime

$600 Billion in 2018

Predicted to reach $3 Trillion by 2020

Source: World Economic Forum

Cybersecurity Spending

$124 Billion in 2019

$188.4 Billion by 2023

Source: Gartner

The Current State of Cybersecurity

Skills Shortage – Not enough trained cybersecurity experts

Labor Intensive “Solutions” require trained cybersecurity experts

New Attack Vectors Get Us To Compromise Ourselves (open source – amplifies sabotage)

Situational awareness is lacking

Top Targets

Government Agencies

Healthcare

Financial Industry

Source: Verizon DBIR 2019

Ransomware

Cryptomining

Credential Theft

Credit Card/Bank Theft

Money

Intellectual Property

Strategic Interests

Malware

Exploits

Phishing

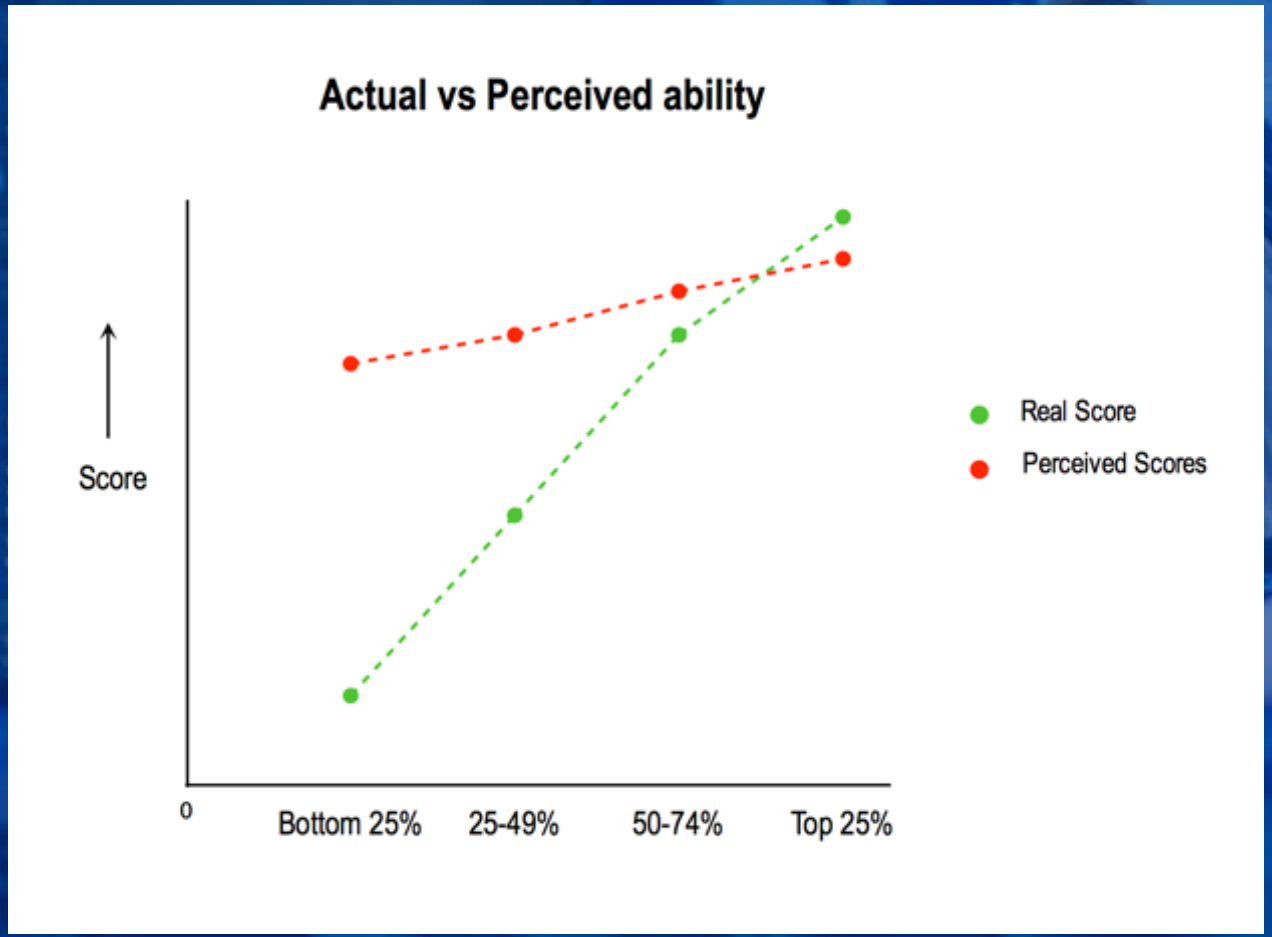
Blended Attacks/Hybrid Attacks

Doc Attacks Malware + Exploits

Emerging — IoT, Cloud


Future State
Where are
we headed?
Cloud
IoT
5G
What happens when attacks jump from
the virtual world to the physical world?

Security is is harder than everyone thinks

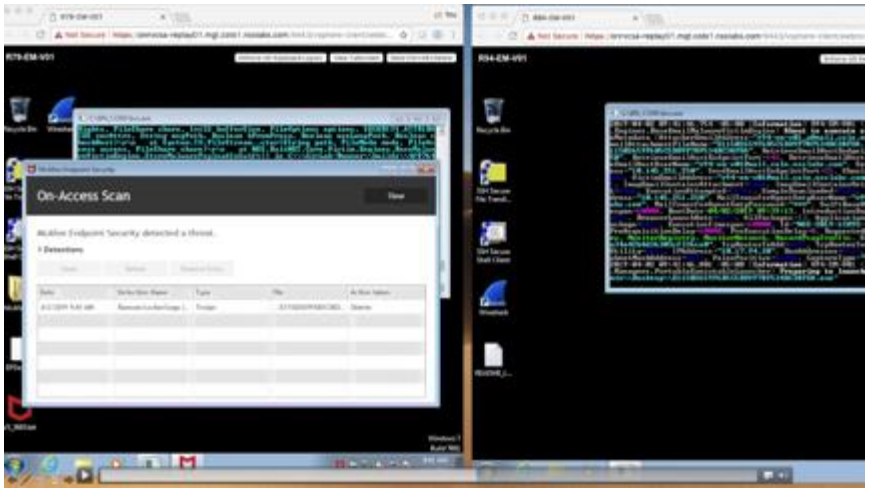


Are We Up for the Challenge?

Test Results Say…

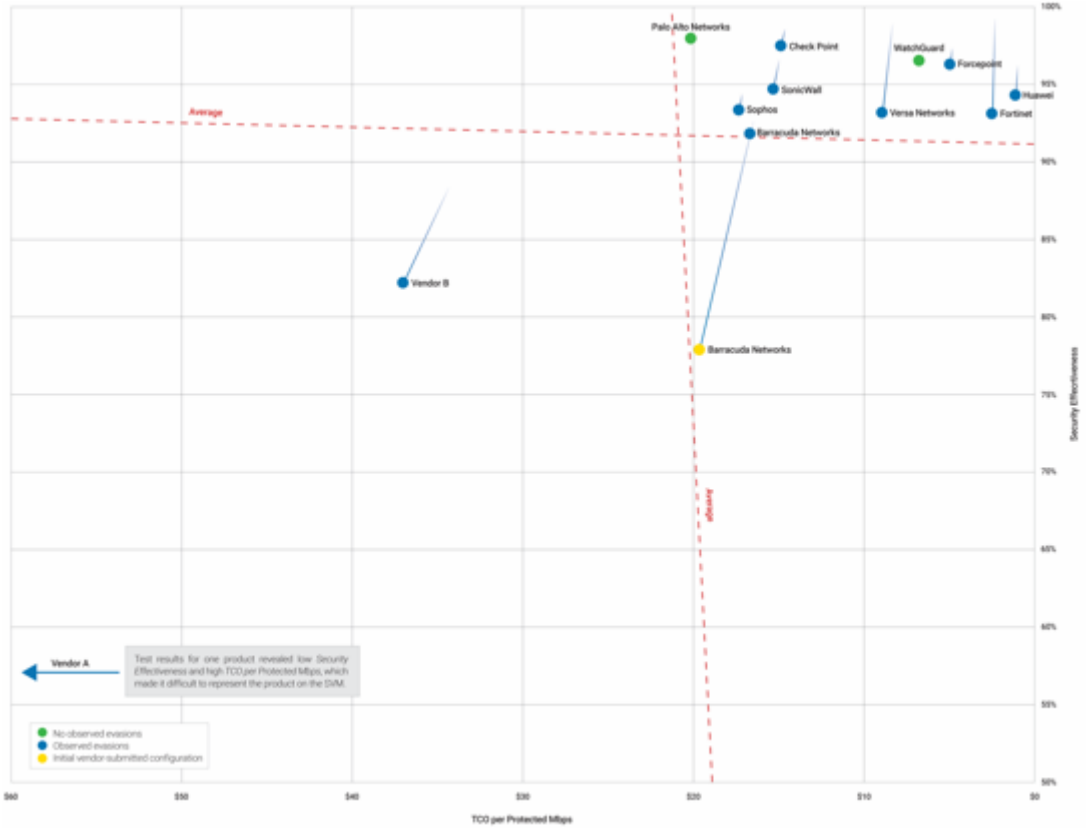
How do you know when a product blocks a known attack, but then fails to stop the same attack when obfuscated?

- **Detailed Test Findings**
  - NGFW Group Test Results
  - Anti-tampering (AEP)
  - BPS Group Test Results



Next Generation Firewall (NGFW) Group Test

- Core to most cybersecurity strategies, yet most easily evaded
- Most widely deployed network security devices
- Enterprises expect NGFWs to prevent exploits and malware from infecting critical systems
- NSS Labs raised the bar this year –
  - Significantly harder test for security effectiveness
  - Exposed weaknesses not seen previously



NGFW 2019 Group Test Results

- **Block Rates** for simple clear text attacks remains strong (over 96%) for 9 of 12 products.
- While known/published exploits are frequently blocked, all 12 products failed **Resiliency** testing (protection library depth). We found we could trivially modify known / blocked exploits and bypass protection in all devices.
- 11 of 12 products failed to block exploits that were obfuscated using **Complex App Layer Evasions** (HTML / Javascript / VBScript).
- **Evasions over decrypted HTTPS** were major problems for Vendor #3. This vendor has been notified and is in the process of fixing the problems.
- NSS Labs tested the ability of NGFWs to properly handle **IP Fragmentation**. We found that despite these evasions having been known and properly handled since the 1990's, they continue to be a challenge for products (for 8 of 12 vendors).

NGFW Failures – Evasion & Resiliency Misses

Vendor	IP Packet Fragmentation / TCP Segmentation	HTTP Evasions	HTTPS Evasions	RPC Fragmentation	URL Obfuscation	FTP / Telnet Evasion	Combonation of Evasions	Advanced Evasions (HTML / Javascript / VBScript)	Resiliency
1	54	0	0	0	0	0	1	16	24
2	0	0	0	0	0	0	0	18	20
3	36	3	16	0	0	0	2	14	17
4	0	2	0	0	0	0	0	48	14
5	19	0	0	0	0	0	0	16	16
6	13	0	0	0	0	0	0	11	15
7	4	0	0	0	0	0	3	1	16
8	0	0	0	0	0	0	0	24	22
9	12	0	0	0	0	0	2	32	23
10	0	0	0	0	0	0	1	7	19
11	23	0	0	0	0	0	1	1	5
12	0	0	0	0	0	0	0	0	10

Anti-Tampering Protection Testing

Introduced as part of the 2019 Advanced Endpoint Protection (AEP) Group Test

- Code-injection vulnerabilities on discovered in 18 of the 21 tested products running on Windows 10.
- Threat prevention successfully disabled in 11 of the 21 tested products.
- The majority of AEP vendors in the test acknowledged the code-injection vulnerabilities and provided fixes to customers in a timely manner.
- To date, 6 new CVEs have been assigned and 1 fix for a previously issued CVE.
- Of the 3 products without code-injection vulnerabilities on Windows 10, they had insecure library loading on Windows 7.

Product Tested (latest versions)	Vulnerable to Code Injection?	Response? Received/Ack'd/Fixed/CVE	Notes
Bitdefender GravityZone Ultra	Yes, Win10 insecure library loading	Yes/Yes/Yes/2019-14242	Fixed in all affected branches/products
Carbon Black CB Defense	Yes, Win10 insecure library loading	Yes/Yes/Yes/No	v3.4.0.955
Check Point SandBlast Next Generation AV	Yes, Win10 insecure library loading	Yes/Yes/Yes/2019-8458	E81.00
Cisco Advanced Malware Protection (AMP) For Endpoints	Yes, Win10 insecure library loading	Yes/Yes/Yes/2019-1932	6.3.3
Comodo Client Security	Yes, Win10 insecure library loading	Yes/Yes/No/0	Unknown
Cylance CylancePROTECT + CylanceOPTICS	Yes, Win10 insecure library loading	Yes/Yes/Yes/0	v1534
Endgame Endpoint Security	Yes, Win10 insecure library loading	Yes/Yes/Yes/0	All versions since 12/31/18
EnSilo Endpoint Security Platform	Yes, Win10 remote thread creation	Yes/Yes/Yes/0	3.0.0.328/3.1.0.316
ESET Endpoint Protection Standard	Yes, Win7 insecure library loading	No/No/No/No	Unknown
Fortinet Technologies FortiClient	Yes, Win10 insecure library loading	Yes/Yes/Yes/2019-6692	6.2.1
F-Secure Computer Protection Premium	Yes, Win10 insecure library loading	Yes/No/No/0	Unknown
G DATA Endpoint Protection	Yes, Win10 insecure library loading	No/No/No/0	Unknown
Kaspersky Endpoint Security For Business	Yes, Win10 insecure library loading	Yes/Yes/Yes/0	KES 11.1
Malwarebytes Endpoint Protection And Response	Yes, Win10 insecure library loading	Yes/Yes/Yes/0	Current Versions
McAfee Endpoint Protection Essential For SMB	Yes, Win10 insecure library loading	Yes/Yes/Yes/2019-3592	5.6.1 HF3
Palo Alto Networks Traps	Yes, Win10 insecure library loading	Yes/Yes/Yes/2019-1577	CVE-2019-1577 is prior report of same issue.
Panda Security Panda Adaptive Defense	Yes, Win10 insecure library loading	Yes/Yes/Yes/0	8.00.14.0002
SentinelOne EPP	Yes, Win7 insecure library loading	Yes/NA/NA/NA	OS Issue
Sophos Intercept X Advanced	Yes, Win7 insecure library loading	Yes/NA/NA/NA	OS Issue
Symantec Endpoint Protection And Advanced Threat Protection	Yes, Win10 insecure library loading	Yes/No/No/0	Unknown
Trend Micro Smart Protection For Endpoints	Yes, Win10 insecure library loading	Yes/Yes/Yes/2019-9492	OfficeScan XG SP1 Build 5383

Summary: Current State of Affairs

- We have a long way to go and we're falling behind
- Threat actors have the upper hand
- We're making things worse by connecting the physical world to the virtual (IoT) using insecure technologies
- The security tools we rely upon to keep us safe are having a hard time keeping up
- If we even have a hope we need situational awareness

Top Targets

Government
Agencies
Healthcare
Financial Industry
Source: Verizon DBIR 2019

Ransomware
Cryptomining
Credential Theft
Credit Card/Bank Theft

Money
Intellectual
Property
Strategic Interests

Malware
Exploits
Phishing
Blended Attacks/Hybrid Attacks
Doc Attacks Malware + Exploits

Emerging — IoT, Cloud

Panel Discussion