THE BAD GUYS ARE WINNING:
Why Your Security Strategy Isn't Working

Nick Cavalancia
Technical Evangelist
Techvangelism
NICK CAVALANCIA

- Technical Evangelist
- Certifications: MVP / MCSE / MCT / MCNE / MCNI
- Co-Founder of ConversationalGeek.com
- Founder of Techvangelism
- Consultant/Trainer/Speaker/Author
- Technical author with over a dozen books
- Technical speaker for Techmentor, Connections, SpiceWorld
- Regular speaker for 1105 Media, Penton, Spiceworks, TechTarget
- Writes, Speaks, and Blogs for some of today’s best-known tech companies
SESSION AGENDA

• Look at the state of security today
• Look at the state of threats today
• Discuss why your security strategy isn’t working
• Provide 3 steps to win the battle
THE STATE OF SECURITY

• Lots of “solutions”
THE STATE OF SECURITY

Source: KnowBe4 2018 Threat Impact and Endpoint Protection Report
THE STATE OF SECURITY

- Lots of “solutions”
- Little focus on strategy
- Feels very reactive
- Not adequately adapting to changes in attack
- Strategy needs to begin with understanding your enemy
STATE OF THE THREAT

- Attacks are becoming more targeted
- Follow the money trail…
  - $8 Billion in Ransomware
  - $6 Trillion in Cybercrime (projected)
- Cybercriminals are focused on new ways to generate “revenue”
- White hats going gray/black
- “Evil”-as-a-Service
STATE OF THE THREAT

- **Malware** – 102% increase in malware volume
- **Ransomware** – 181.5M ransomware attacks
- **Encrypted Attacks** – 275% increase
- **Cryptojacking** – 5.6M CoinHive attacks
- **Evasive Malware** - 86% of exploit kits, 85% of payloads

WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number. SCAM.

WAIT FOR IT
Enter your bank account number. SCAM.

THERE IT IS
Enter your bank account number. OKEY-DOKEY.
CYBER ATTACKS: A CLOSER LOOK

Initial Access → Data Breaches

→ Ransomware

→ Cryptojacking

→ Fraud
# THE STATE OF SECURITY

Source: KnowBe4 2018 Threat Impact and Endpoint Protection Report

<table>
<thead>
<tr>
<th>Protection Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>72%</td>
</tr>
<tr>
<td>Email Protection</td>
<td>61%</td>
</tr>
<tr>
<td>Endpoint Protection</td>
<td>59%</td>
</tr>
<tr>
<td>Advanced Threat Protection</td>
<td>37%</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>36%</td>
</tr>
<tr>
<td>Endpoint Detection &amp; Response</td>
<td>30%</td>
</tr>
<tr>
<td>Next-Gen AV</td>
<td>27%</td>
</tr>
<tr>
<td>Application Whitelisting</td>
<td>26%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>
With so much security in place, why are we still experiencing attacks?
THE PROBLEM WITH SECURITY

• Not Layered
• Doesn’t Align with the Attack
• Not Leveraging AI / Machine Learning
• Not Optimized
STEP 1: START WITH DEFENSE IN DEPTH
USING A LAYERED SECURITY STRATEGY
USE AN ATTACK-CENTRIC SECURITY STRATEGY

- Perimeter: Vulnerabilities, Email, Web, Phone
- User: Phishing, Scams, Social Engineering
- Endpoint: Malware, Evasive Techniques, Fileless, RDP
- Identity: Leveraging Credentials, Lateral Movement
- Privilege: Elevation, Permissions, Persistence
- Apps: Recon, Leverage, Access
- Data: Exfiltration, Encryption, Fraud, Espionage
GETTING TO DEFENSE IN DEPTH

- **Perimeter**
  - Firewalls, Email Scanning, DNS Filtering, Web Scanning
- **User**
  - Security Awareness Training
- **Endpoint**
  - AV, EDR, Application Whitelisting, EMM
  - MFA for EVERYONE
- **Identity**
  - PAM, PSM
- **Privilege**
  - App-specific Auditing, UAM, UBA
- **Apps**
  - UAM, File Auditing

Delivered by KNect365
TMT: an Informa business

#ITDEVCONNECTIONS | ITDEVCONNECTIONS.COM
HOW MUCH TRUST SHOULD YOU HAVE?
STEP 2: LEVERAGE AI/ML
THE VALUE OF MACHINE LEARNING

• Instant expertise
• Adaptive expertise
• Extends intelligence beyond your organization
• Improves protection through sharing
STEP 3: OPTIMIZE YOUR STRATEGY
WINNING THE BATTLE

• Map the strategy to the state of attack
• Checklist of Solutions ➤ Defense in Depth
• Leverage intelligence through machine learning
• Consider an adaptive strategy
QUESTIONS?
THANK YOU

nick.cavalancia@techvangelism.com

Don’t forget to visit conversationalgeek.com