



4 KEYS to STOPPING RANSOMWARE

TCEA

CONVENTION & EXPOSITION

Feb. 4-8, 2019 | San Antonio, TX

RANSOMWARE EPIDEMIC



Roseburg school district continues work to repair servers after ransomware attack

Cloquet school district hit by second ransomware attack

Connecticut School District Hit with Ransomware Attack

A ransomware attack and no contingency plan cost a Massachusetts school district \$10,000

Keys public school computers remain down a 5th day after cyberattack

K-12 Cyber Incident Map

WHY IS THIS HAPPENING

Ransomware allows attacks to be fully automated.

- \$10 kit on Dark Web = \$100k revenue
- 45,000 kits available
- \$750 ransomware bundle – includes tips

30%-60% of those infected are paying the ransom.

- Gartner research note on how to pay.

No lack of victims.



WHY IS THIS HAPPENING

Targeted Attacks

Disruption

SamSam Indictments:

"The defendants did not just indiscriminately 'cross their fingers' and hope their ransomware randomly compromised just any computer system. Rather, they deliberately engaged in an extreme form of 21st-century digital blackmail, attacking and extorting vulnerable victims like hospitals and schools, victims they knew would be willing and able to pay.



HOW IS THIS HAPPENING?



Lack of Awareness/Employee Carelessness

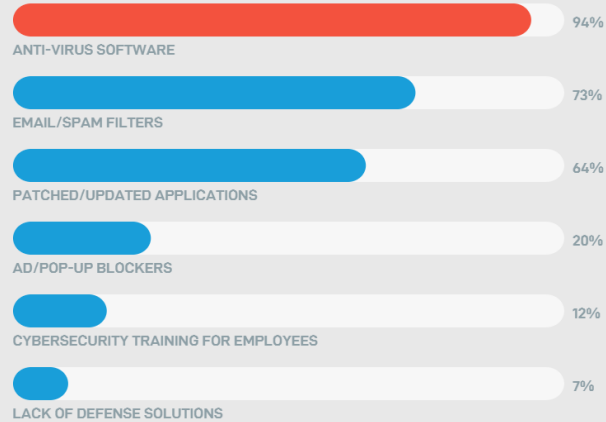
64% of working adults don't know what Ransomware is.
(Wombat Security Research)

Phishing becoming more sophisticated.

Equifax, Facebook and other stolen data.

HOW IS THIS HAPPENING?

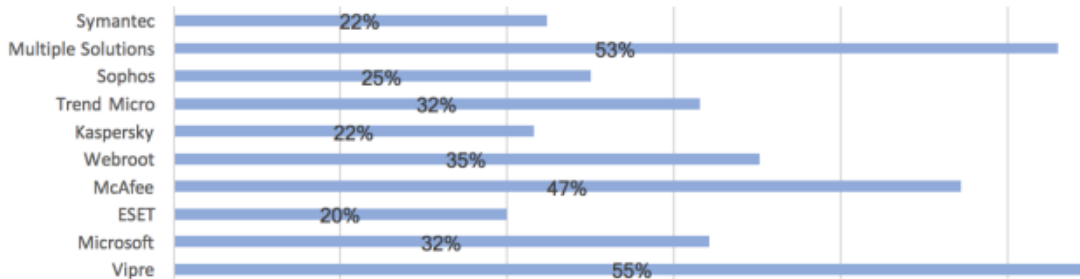
The failure of traditional Anti-Virus software/endpoint security.



Of the ransomware incidents you've encountered, had they implemented any of the following? (Check all that apply)

As no single solution is guaranteed to prevent ransomware attacks, a multilayered portfolio is highly recommended.

Percentage of organizations experiencing a ransomware attack (by AV solution)



A MASSIVE SECURITY HOLE



Most traditional Anti-virus software is based on outdated “black list” approach to prevention.

- 99% of malware hashes are seen for only 58 seconds or less.
- Most malware is only seen once.

BLACKLISTFLAWS



Obsolete

Created in the 80s to stop viruses from spreading, the black list has proven wholly ineffective against polymorphic viruses and ransomware.



Reactive

By design, an infection must occur before a virus can be added to the list. The black list is reactive, and guarantees the world will always have viruses.



Slow

Antivirus makers have added "features" such as heuristics and vulnerability patches, which reduce the attack surface at the expense of system performance.



Foreign Made

The explosion of threats has made the black list expensive to maintain forcing black list antivirus makers offshore to improve profits.



Ineffective

As the ransomware menace gains traction, we are at a crossroads on how much longer we can stand the black list antivirus's inferior security.

WINDOW OF INFECTION



Most traditional Anti-virus software is based on outdated “black list” approach to prevention.

- 99% of malware hashes are seen for only 58 seconds or less.
- Most malware is only seen once.

WHAT IS NEXT

- Increasing number that pay ransom – Do not get their data back. (1 in 5 never get data back)
- Reinfection rates beginning to skyrocket.
- Back Ups are becoming infected with greater frequency.
- Ransom sweet-spot has been found.



4KEYS

EndUser Training

- Testing
- 3rd party

Back Ups

- Testing
- Best Practices

Patching


- Windows Updates
- Frequency

Endpoint Protection

- Application Whitelisting
- Fileless Malware Protection
- RDP



WHITELIST SECURITY

A man in a black jacket stands at the entrance of a building, looking at a line of people waiting outside. The line is formed by a series of black stanchions connected by a dark rope. The people in the line are diverse in age and appearance, and they are all looking towards the entrance. The background is a red brick wall.

Control over programs that are allowed to execute on a computer. If the program or software isn't on the whitelist, the program is not allowed to execute.

Application whitelisting is not new. Knock against Application whitelisting has been manageability.



FILELESS INFECTIONS

Fileless infections are a method of attack where a script is run through a legitimate scripting engine such as Powershell. Since no bad file is ever executed, it renders the black list approach useless.

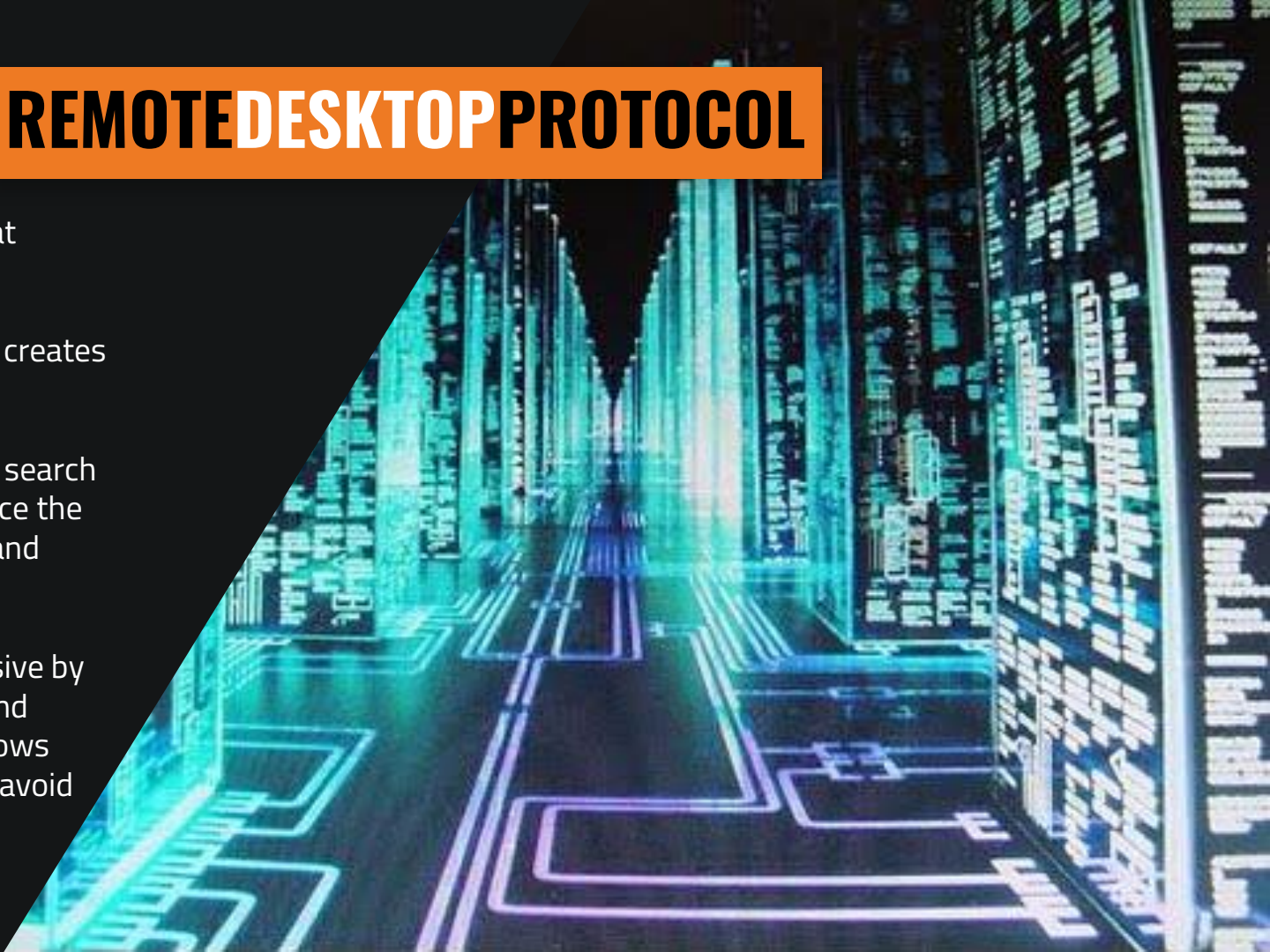
Layered on top of PC Matic's white list, we have developed a technology to block the bad scripts without blocking any good ones.

REMOTE DESKTOP PROTOCOL

RDP is a critical IT feature that allows remote access and management of servers and desktops. Sadly, this feature creates a security hole.

Hackers have automated the search for open RDP ports, brute force the password, disable antivirus, and deploy ransomware.

PC Matic counters this offensive by displaying open RDP ports, and automatically modifies Windows account lockout threshold to avoid brute force attacks.





WHY PC MATIC?

Advanced Technologies

- Proactive Whitelist Architecture
- Fileless Infection Heuristics
- RDP Reporting and Protection
- Cloud Console

Superior System Performance

- Lightweight (20 MB memory, <1% CPU)
- Faster file download times
- Faster web browsing
- Faster application install times
- Faster application run times
- Faster file copy

Operating Systems

- Windows XP, Vista, 8, 10
- Windows Server 2008, 2012, 2016
- Android

ANTIVIRUSTESTING



*Highest Detection Rates in History of
Virus Bulletin RAP Test*



*100% Detection of over 5,000 malware samples
Jan/Feb 2018*



*PC Mag Malware Protection Test
The only product to detect 100%
August 2017*

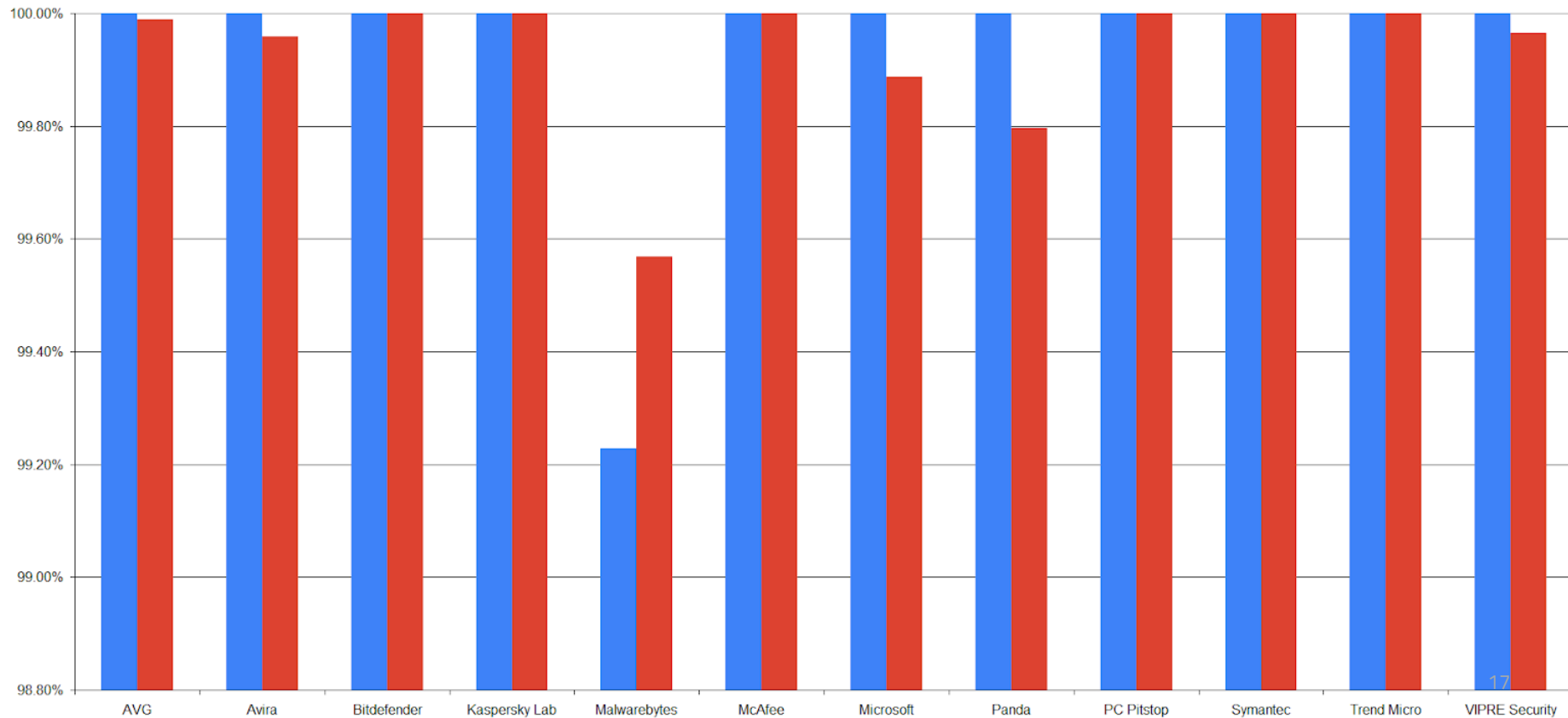
ANTIVIRUS DETECTION TESTING



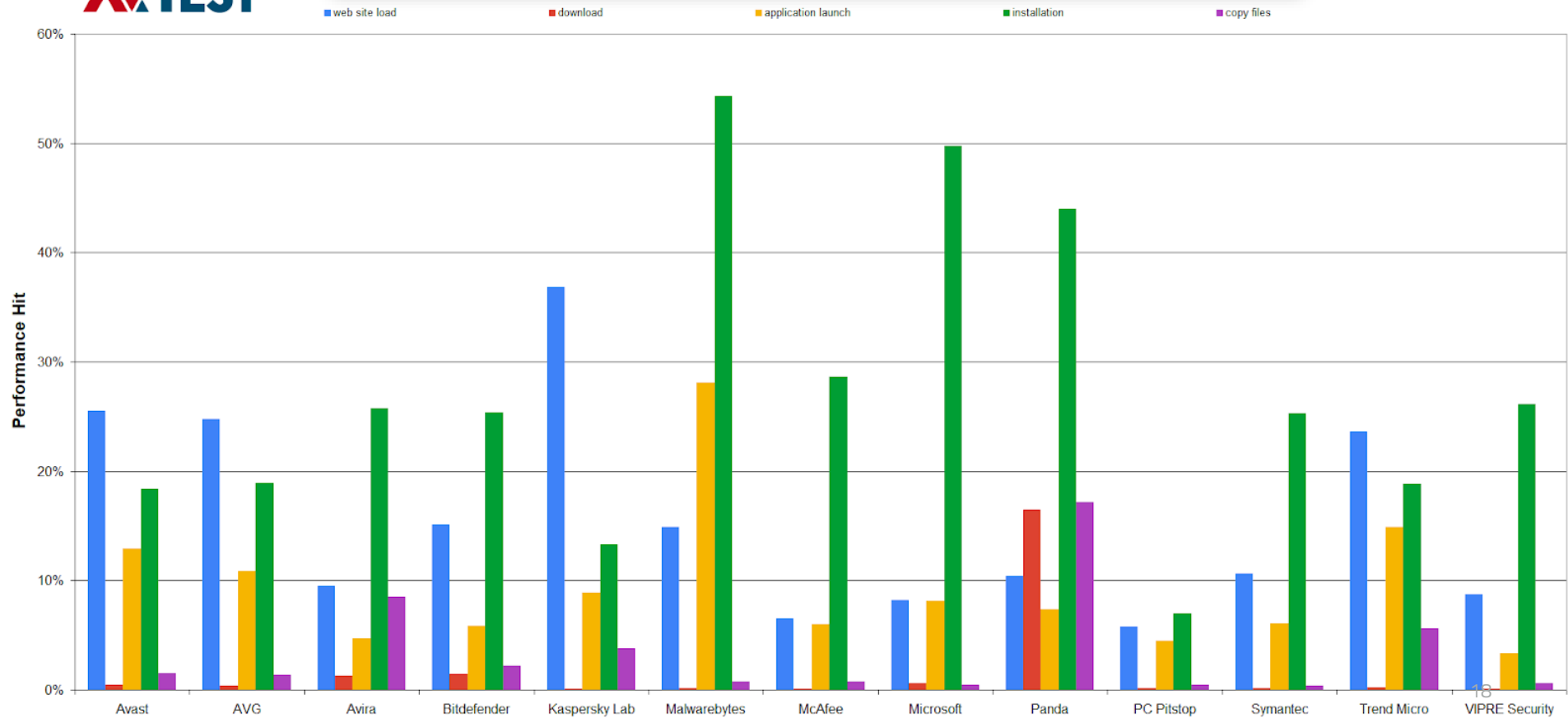
Detection Rates (Jan 2019)

■ Real World Attacks (259)

■ Prevalent Malware (19697)



Performance (Jan 2018)



MADE IN AMERICA

PC Matic is the **only** anti-virus software that is developed, researched and supported – **exclusively** in the United States.

Top 5 Cybersecurity Trends

“Security buying decisions are increasingly based on geopolitical concerns” - Gartner



QUESTIONS?

Email corey@pcmatic.com for a copy of this presentation.