Securing our Schools

PC Matic PRO

Large Payments & Lost Servers

Los Angeles Valley College, Los Angeles CA
The infection began during the winter enrollment period and locked down their network in addition to the email and voicemail systems. After 6 days of deliberation, a $28,000 payment was made in bitcoin and the decryption key was used to recover previously locked data.

Horry County Schools, Myrtle Beach SC
Finding it's way in through an outdated server, several systems across the district were affected including school lunch payments. Even with backups of their systems, HCS elected to avoid long restoration times and pay the $10,000 ransom.

Swedesboro-Woolwich District, Swedesboro NJ
On a regular Saturday morning the network went down and a ransom message appeared on computers asking for around $125,000 in payment. Email servers and their cafeteria lunch ordering system had to be wiped clean and rebuilt to remove the malware and avoid paying the ransom.

Education has become one of the most frequently targeted and vulnerable industries to malware and more specifically ransomware. With a large amount of users, devices, and reliance on technology, schools are particularly appealing to cyber criminals.

When one infection is able to spread to a large amount of devices it often leads to a higher ransom request. Cyber criminals know that many school districts will weigh the money lost recovering with backups and just pay the ransom to regain access to their data faster.

Are Schools a Cyber Criminal's Best Friend?

- In a recent survey by BitSight Insights, it was found that Education has quickly become the most targeted sector by ransomware cyber criminals. Of the 2,100 schools surveyed almost 14% have experienced ransomware in the last 12 months, three times more than Healthcare and ten times more than Finance.

- According to Will Bales, a special agent in the FBI's cyber division, "Ransomware does not discriminate, whether it's a big school district or a small school district, they have the same possibility of being hit."

- Cyber criminals have begun to create new methods to access school technology, cold calling schools posing as department of education officials looking for teacher emails. The subsequent email contains ransomware the criminal hopes to unleash inside the school's network.
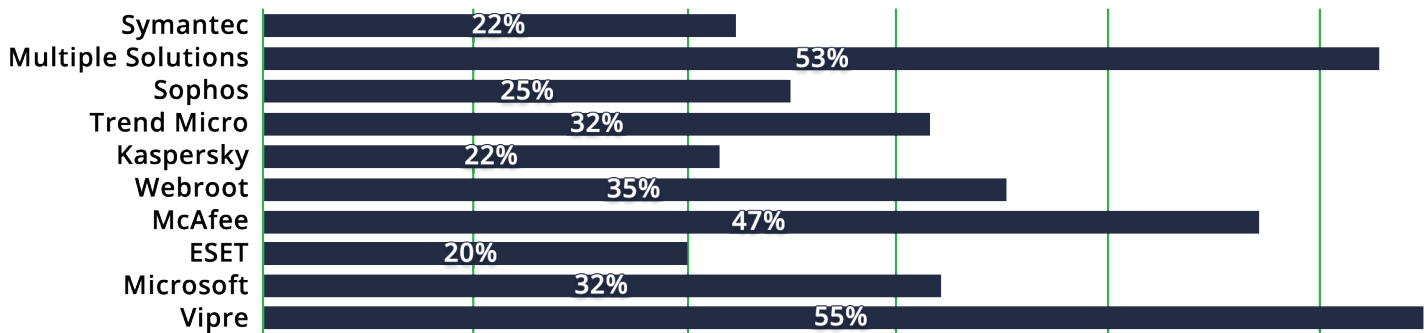
⊕ pcmatic.com/pro
✉ info@pcmatic.com
☎ 855-865-6655

Legacy Antivirus Has Failed

The amount of ransomware variants that are being introduced into the world on a daily basis is staggering, and it's not surprising that the traditional blacklist approach can't keep up. In a recent survey by KnowBe4 you can see the percentage of organizations experiencing a ransomware attack by current AV solution.

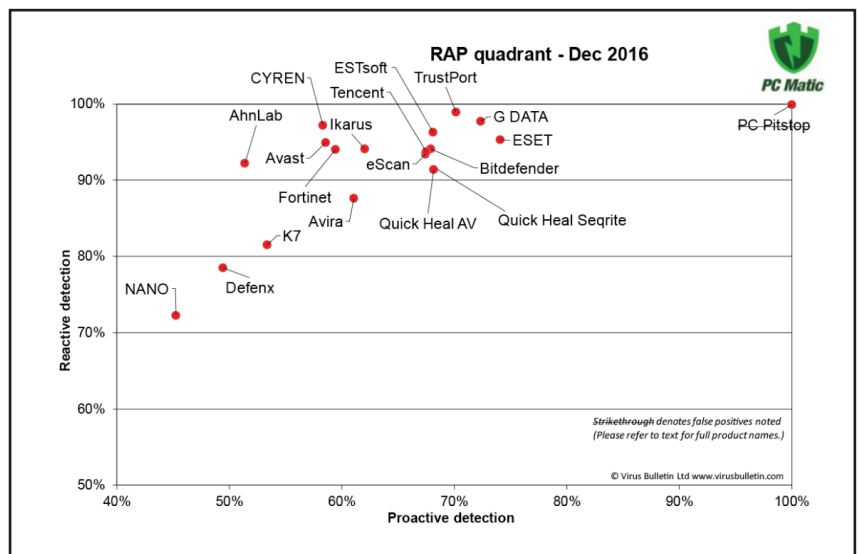## Percentage of organizations experiencing a ransomware attack (by AV solution)

AV Solution	Percentage
Symantec	22%
Multiple Solutions	53%
Sophos	25%
Trend Micro	32%
Kaspersky	22%
Webroot	35%
McAfee	47%
ESET	20%
Microsoft	32%
Vipre	55%

*KnowBe4 Survey of 500 Organizations May 2017

A New Approach is Desperately Needed.

With PC Matic Pro we are providing default-deny application whitelisting on a global level, which removes the overhead needed to implement a whitelisting solution and maintain it over time.

We stop all unknown software from executing on the endpoint and only allow known good applications that are on our whitelist.

You don't have to take our word for it; independent testing houses are testing security products frequently to see how effective they actually are. If products you're considering aren't routinely tested it's important to ask why. We offer up one recent test of our product here from Virus Bulletin to begin your deep dive into detection rates.

RAP quadrant - Dec 2016

Strikethrough denotes false positives noted
(Please refer to text for full product names.)

© Virus Bulletin Ltd www.virusbulletin.com