# Defeating Ransomware in K-12

PC Matic PRO

## Targeting the Education Vertical

According to industry experts, the Education vertical remains most likely to suffer a ransomware attack. This is due in part to cyber criminals targeting the vertical, and a lack of funds, lack of staff, or both.

Leaving vulnerable holes in the network can lead to cyber criminals with a broad net infecting entire schools with a ransomware attack. Ransom demands can be in excess of ten to twenty thousand dollars depending on the scale of the infection.

### Dark Overlord

A notorious hacking group launched a campaign against several school districts around the USA stealing student, teacher, and parent information before encrypting it.

The group then targeted parents with increasingly threatening text messages and phone calls about the school children. Schools closed for days to assess the threat to students and faculty. After no negotiation or payments from the schools, student personal information was released online.


## How easy could it be for criminals?

- Anyone can buy a ransomware as a service kit on the dark web for $10 and generate upwards of $100,000.

## Where is Ransomware Headed?

- Industry experts predict that ransomware will begin to steal personal information before encrypting it, and then not only use it to extort the victims further, but sell it on the dark web.

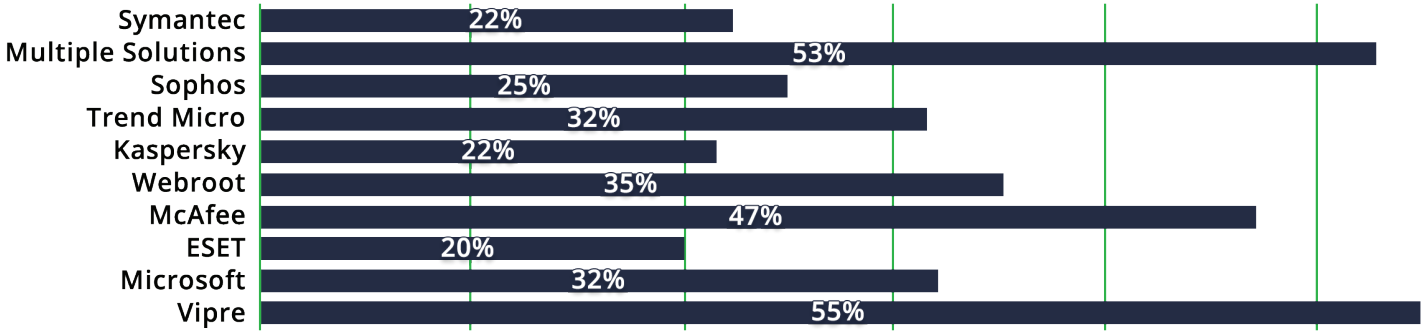
- This gives them another leverage point over the victim and another way to make money if ransoms aren't paid. Before you think this sounds too far fetched to actually start happening...

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)**




*KnowBe4 Survey of 500 Organizations May 2017

## Shift The Approach to Prevention.

PC Matic Pro is providing default-deny application whitelisting on a global level, which removes the overhead needed to implement a whitelisting solution and maintain it over time. With our solution the focus is shifted to prevention instead of detection and remediation. We stop all unknown software from executing on the endpoint and only allow known good applications that are on our whitelist.

In 2017...

| 4,000+ | $5 Billion | 7,000 | 40 sec |
|---|---|---|---|
| Ransomware attacks per day | In total damages throughout the year | Number of Student PII data released | Time between each ransomware attack |

**Customer Success Stories:**
Houston County Schools

"I'm dealing with 6,400 students, and about 700 teachers, administrators and support people that are using their computers daily. I need to make sure bad things are blocked and good things are allowed to come through, especially for teachers. They need it to work properly and not give any hiccups during the time it's running. It's a big deal to us that it runs smoothly. PC Matic Pro has done a very good job for us."

*– Bob Blalock Technology Coordinator, Houston County Schools*