State & Local Government Security

PC Matic PRO

Ransomware Stops Critical Systems

Licking County, Ohio

After a ransomware attack struck the county offices, online services and office telephones for the local government were taken down for at least a week. 911 dispatch in the county was forced to work without office phones or computers but assured residents emergency services were still available.

Newark, New Jersey

The city of Newark's computers were taken down for the second time in two years due to a ransomware attack. This time the attackers demanded $30,000 in bitcoin to decrypt the files. The CIO for the city said, "The virus compromised our network and disrupted many services that we offer, our police services are unaffected and continue operating normally..."

Murfreesboro, Tennessee

The emergency services in Murfreesboro were hit with a ransomware attack earlier this year that took their systems offline. Two servers and nineteen endpoints were affected by the WannaCry outbreak and the data on them was unretrievable.

Cyber criminals have begun to specifically target those who protect us with specific types of ransomware or campaigns. A ransomware campaign using CryptFile2 recently focused mostly on State and Local government by a factor of ten. Criminals know that many governments, especially small ones, won't be as equipped to defend against attacks.

Ransomware has been noted as the top concern among local governments in a recent study and a better approach is desperately needed. PC Matic Pro takes a strong stance against ransomware with a default-deny approach based on our globally automated whitelist. We always stop unknown applications from running including even the newest ransomware.

Cyber Criminals Wage War on State & Local Governments

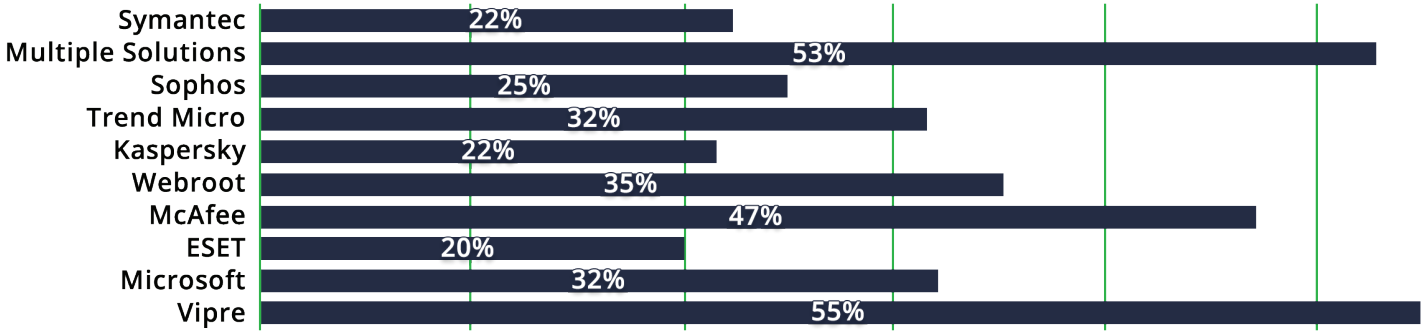
- According to cyber security experts, new variants of ransomware like MarsJoke have been introduced to specifically target state and local government agencies in their infection campaigns.
- Even if governments can avoid paying the ransom, downtime can often be more costly to the taxpayer. San Francisco's SFMTA was infected and payment systems went down for public transport. To avoid downtime free rides were offered as they scrambled to restore the systems. This lead to a huge cost for SFMTA and further demonstrates why prevention, not reaction, is key.
- Ransomware is expanding at a blistering pace according to statistics from the US Government. 2016 saw more than a 300% increase in attacks compared to 2015; and this year is set to continue the trend.

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)

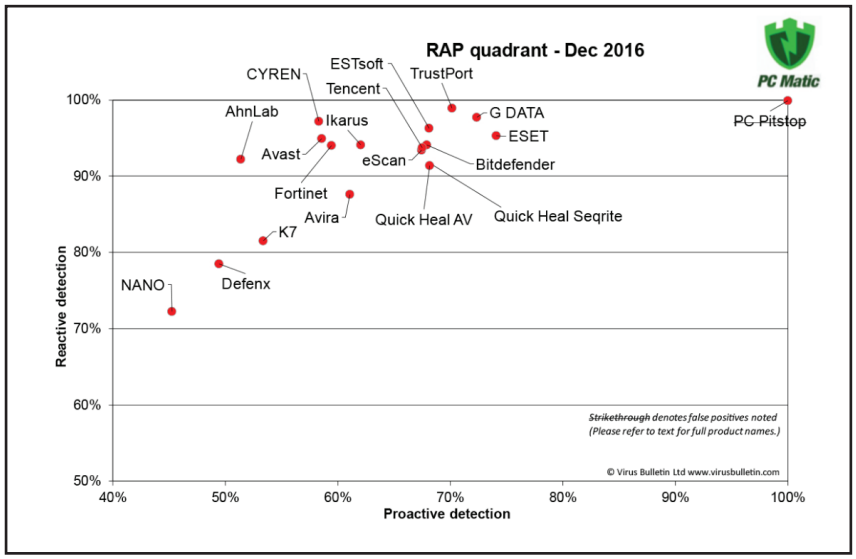


*KnowBe4 Survey of 500 Organizations May 2017

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.



Customer Success Stories:
Dawes County Sheriff

"With nearly 10,000 citizens depending on Dawes County Police to protect them, it's critical that Sheriff Dailey's systems are up and running 24/7. "As most people know, the internet is ripe with hazards. Because of the nature of how we use our computers, for very detailed and personal information, we needed to protect it as best we could. I'm tickled to death with it. I really like it. We've had zero problems with our machines, since we put it on."

– Karl Dailey, Dawes County Sheriff