DEEPARMOR®

Discussing the Ransomware Crisis Facing State and Local Governments

State and local governments are systematically targeted with ransomware developed and distributed by international criminal organizations. Worldwide, nearly 70% of state and local government networks have been breached by ransomware or other cyber-attacks, with 200 million government records compromised worldwide in the first half of 2016 alone. These attacks have become increasingly common in every kind of government agency, including utilities, police departments, educational institutions, and 911 centers.

Local government agencies are not only high value targets, but often soft targets due to outdated technology infrastructure—and hackers know this. By attacking government entities, hackers can gain access to such valuable and classified information as national ID numbers, fingerprints, confidential documents and emails, passwords, credit card numbers, and more.

Once they've seized control of a system, hackers will often demand a ransom to be paid in cryptocurrency or post compromised information on the dark web to be sold to the highest bidder. Here are three recent examples.

Forbes NOV. 2016

Ransomware Crooks Demand $70k after Hacking the SF Transport System

Ransomware infected computers at San Francisco's Municipal Transportation Agency, with hackers demanding roughly $70,000 to release the system. MTA was unable to ticket passengers and so took a huge financial hit for several days before their systems could be cleaned. The hackers have also threatened to leak 30GM of the MTA's data.

Detroit Free Press APRIL 2016

Lansing Utility Paid $25k Ransom after Cyberattack

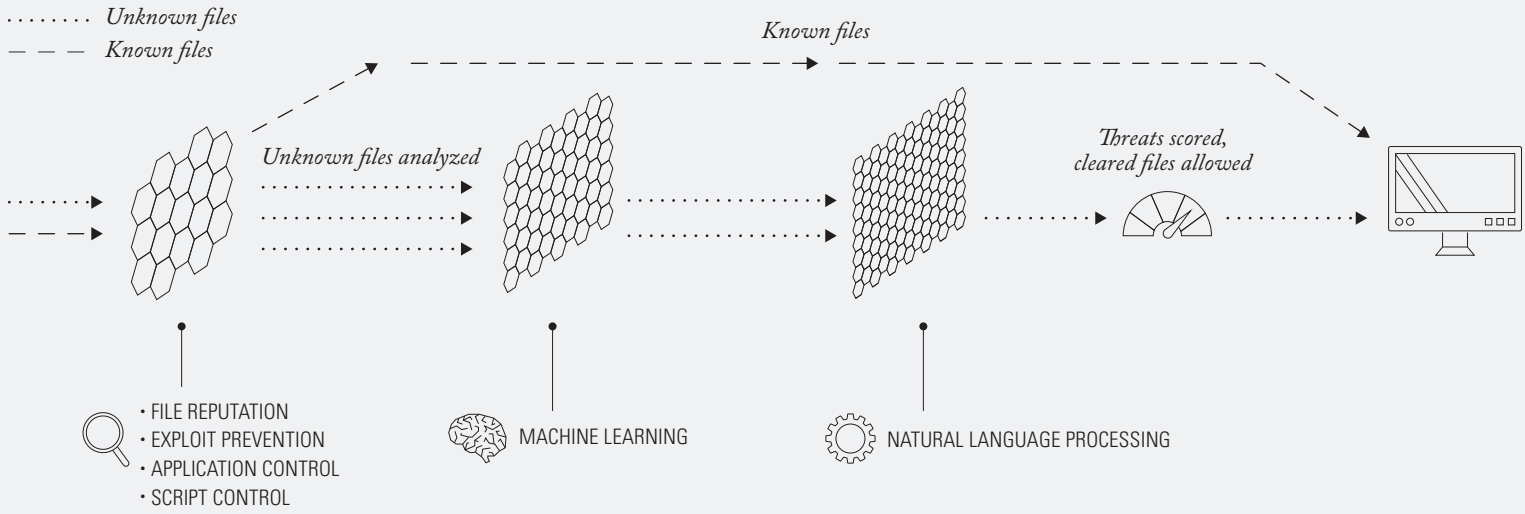
A cyberattack on the Lansing Board of Water & Light, transmitted via an infected email, forced the board to pay a $25,000 ransom to unlock its email systems and phone lines after they were disabled by a cyberattack. The attack took a week to recover from, and beyond the ransom, its full cost is estimated at $2.4 million.

Newark **Advocate** JAN. 2017

Cyber-attack Cripples Licking County Government

A computer virus forced Licking County to shut down systems in government agencies throughout the county in an effort to keep the virus from spreading further and to protect their data. Dispatchers at the 911 Center had no computer access, the courts had no working phones or computers, and the DMV and Department of Job and Family Services had no working phones.

How DeepArmor Works



DeepArmor is not just a logical solution to this threat—it's an imperative to mitigate the financial and operating risks associated with the ransomware crisis.

4x Better Protection

Machine learning malware engine provides 4x better protection from zero-day and polymorphic threats (e.g., ransomware) vs. traditional endpoint security solutions

66% Faster Response

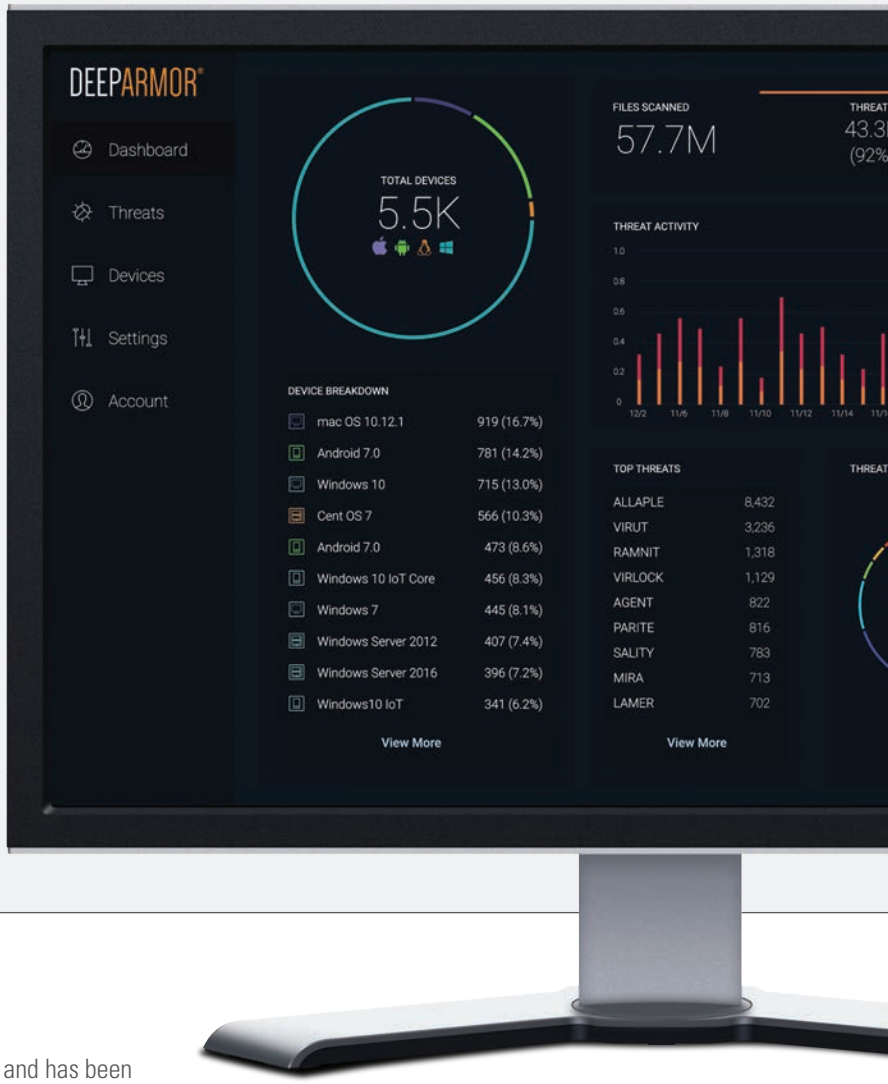
NLP-based threat intelligence and automated threat research can reduce alert analysis time by 66%, leading to faster response and remediation

Reduce Risk

Ransomware attackers typically demand one bitcoin per device (currently $1,037) to decrypt the user's files, DeepArmor costs a fraction that for a one-year subscription

Lower TCO

Cloud-based, security as a service architecture reduces upfront deployment costs and overall TCO



Don't Wait Until You're a Victim

DeepArmor Enterprise is a per device, per year subscription service and has been specifically trained on ransomware strains attacking state and local governments.

About SparkCognition

Austin, Texas-based SparkCognition develops cutting-edge machine learning that models physical and virtual assets, continuously learns from data, and derives intelligent insights to secure and protect infrastructure around the clock. The company's cybersecurity solutions analyzes structured and unstructured data and natural language sources to identify potential attacks in the IT and IoT environments. The uniqueness of the cognitive platform is underscored by the fact that it can continuously learn from data and derive automated insights to thwart emerging issues, without the need to build manual models.

Learn More About DeepArmor®

To learn more about how SparkCognition's DeepArmor can add a cognitive layer to improve your security posture, please email **sales@sparkcognition.com** or request a demo on our website **www.sparkcognition.com/deeparmor**