sparkcognition™ EPP

How MSSPs can Thwart the Ransomware Crisis

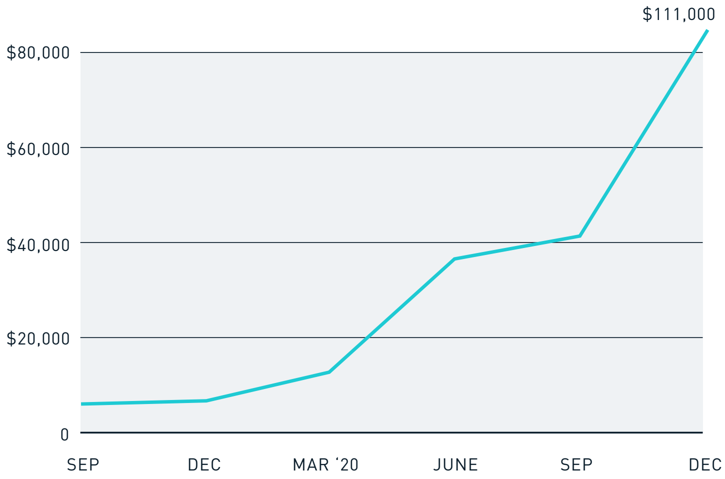
For the last several years, a quiet crisis has quickly become the predominant threat to businesses, governments, and even individual consumers. While cyberattacks vary from case to case, the general sequence is as follows. First, hackers obtain access to key assets like core databases. Next, they encrypt these assets, rendering them unavailable to the organization. Finally, they demand that a ransom be paid in cryptocurrency, or post compromised information on the dark web to be sold to the highest bidder.

The Colonial Pipeline attack, orchestrated by a criminal organization called DarkSide, dominated the news in May of 2021. This attack, which began with the encryption of key business assets, was quickly followed by a ransom demand, leading Colonial Pipeline to shut down the largest fuel pipeline in the U.S. for 11 days. As a result, gasoline prices hit their highest levels in seven years, many gas stations were completely depleted, and a state of emergency was declared in several states. This attack demonstrated the critical importance of protecting more than just traditional IT assets, like servers and computing endpoints. Today's cyber criminals can target and reach exposed operational and industrial assets, too.

This may not fully represent the exponential growth of ransomware, because for every victim of ransomware that reports an attack, there are many more who quietly pay the ransom without notifying authorities.

Heading into 2022, the threat posed by ransomware is expected to get worse, not better. According to Fintech News, the average ransomware payment in 2020 increased by a third over 2019. Boston-based cybersecurity firm Recorded Future cites more than 65,000 ransomware attacks in the U.S. in 2020. On average, that's more than seven incidents per hour.

FIGURE 1: Average Ransomware Payment as of Q4 2020



Source: Fintech News

Paying the ransom is only a fraction of the cost businesses face when they are hit. Business downtime, network cost, repair and replacement of devices, and lost opportunity, totaled with the ransom, add up to staggering costs for ransomware victims. In addition, hackers now see individuals as easy targets, and unsuspecting consumers increasingly find themselves on the receiving end of ransomware attacks.

More ransomware attacks in the news.

BBC NEWS | FEB. 2020
ISS World hack leaves thousands of employees offline

A ransomware attack on Danish facilities management company ISS World forced the firm to take its entire IT network offline, massively disrupting business functions. A month later, ISS World was still working to relaunch business-critical systems with reduced functionality, and stated it expected restoring and rebuilding its systems to take until the end of 2020. The total cost of the incident is still ongoing, but is estimated at between $75 to $112.4 million.

THE WALL STREET JOURNAL | JAN. 2020
Travelex paid hackers multimillion-dollar ransom before hitting new obstacles

Foreign currency exchange business Travelex was crippled by a ransomware attack, requiring it to take its websites, app, and IT network offline to try to combat the virus. The company was unable to resume business for almost two months. To protect customer data, Travelex was forced to pay a ransom of $2.3 million in Bitcoin.

THE GUARDIAN | FEB. 2020
Ransomware attack leaves council facing huge bill to restore services

The local government of Redcar and Cleveland in northeast England suffered a devastating cyber attack that disabled its servers for three weeks, with council staff forced to rely on pencil and paper. The council was left barely able to function, and in the aftermath faced costs of between £11 to 18 million—well above its entire budget for 2020 and 2021—just to repair the damage, leaving citizens in fear that their local government may be "in danger of collapse."

A NEW MODEL OF PROTECTION WITH AI

In this evolving threat landscape, businesses, governments, and individual consumers need a new approach to protect them from sophisticated cybercriminals. That's why SparkCognition developed a next-generation cognitive endpoint protection solution, the SparkCognition™ EPP product portfolio. These solutions use the power of artificial intelligence (AI) and deep learning algorithms to analyze executables, scripts, DLLs, and documents, assess them for threat potential, and then take action to block or mitigate a possible security breach.

Instead of using signatures, heuristics, or rules-based approaches to detect threats, SparkCognition EPP exclusively uses AI to prevent file-based, fileless, and in-memory attacks.

- **Close the protection gap left by legacy antivirus**

  Cognitive endpoint protection delivers more effective protection compared to signature-based anti-malware solutions—especially when dealing with zero-day attacks. Patented machine learning algorithms protect you from the 400M+ new malware variants discovered each year.

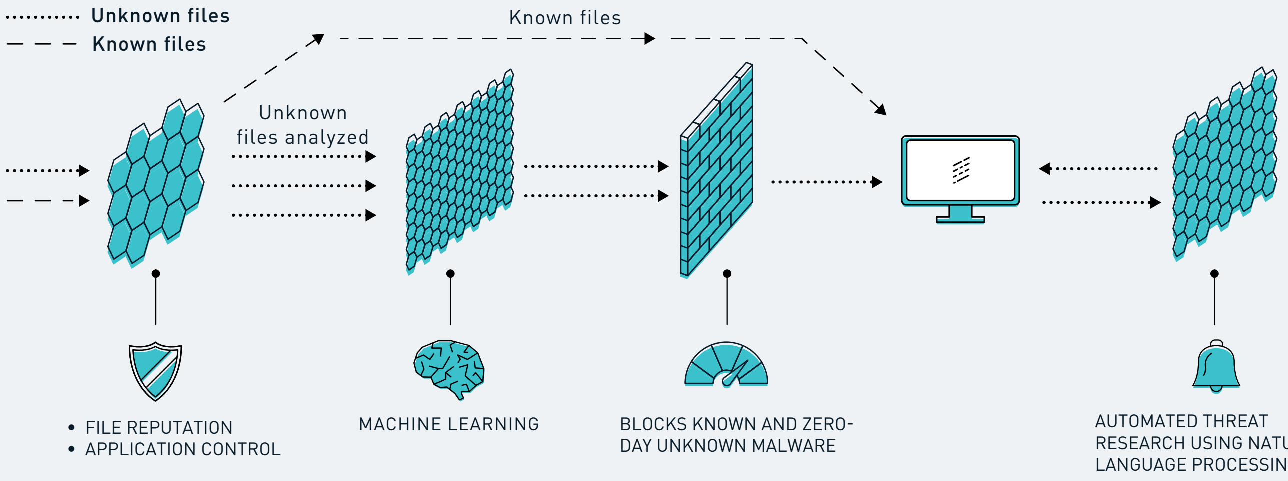
- **Detect weaponized document attacks**

  SparkCognition EPP helps protect against weaponized documents by applying AI analysis to determine the threat potential of files like PDFs and Microsoft Office documents without using signatures, heuristics, or rudimentary control features.

- **Save time, effort, and money**

  SparkCognition EPP's cloud-hosted architecture helps reduce upfront deployment costs and overall total cost of ownership compared to on-prem solutions.

FIGURE 2: How SparkCognition EPP Works



SparkCognition EPP is the best solution to mitigate the financial and operating risks associated with the ransomware crisis.

DON'T WAIT FOR YOUR CUSTOMERS TO BECOME VICTIMS

Learn how you can easily integrate SparkCognition EPP into your Managed Security Services portfolio, driving incremental revenue, reducing operational impact, and bringing cutting-edge cognitive AI protection to your customers.

Contact us for a demo today at info@sparkcognition.com.

ABOUT SPARKCOGNITION

SparkCognition's award-winning AI solutions allow organizations to predict future outcomes, optimize processes, and prevent cyberattacks. We partner with the world's industry leaders to analyze, optimize, and learn from data, augment human intelligence, drive profitable growth, and achieve operational excellence. Our patented AI, machine learning, and natural language technologies lead the industry in innovation and accelerate digital transformation. Our solutions allow organizations to solve critical challenges—prevent unexpected downtime, maximize asset performance, optimize prices, and ensure worker safety while avoiding zero-day cyberattacks on essential IT and OT infrastructure. To learn more about how SparkCognition's AI solutions can unlock the power in your data, visit www.sparkcognition.com.

Contact SparkCognition today at info@sparkcognition.com