Malwarebytes

CASE STUDY

# East Irondequoit CSD claims victory over Emotet Trojan

**It's not often a school district can create a model for modernizing teaching pedagogy through digital transformation while also successfully weathering a pervasive Trojan infection on the first week of school. East Irondequoit Central School District—serving approximately 3,200 students across six schools in Monroe County, New York—did just that.**

## Achieving teaching excellence through digital conversion

The East Irondequoit Central School District leadership team believed that thoughtful integration of current technologies had the potential to fundamentally shift how instruction could be facilitated in the classroom. With this in mind Joseph Sutorius, Chief Information Officer for East Irondequoit CSD, and his team began equipping the faculty and students with 3,400 iPads and Windows laptops and ultimately helped foster the creation of modern-teaching spaces with unlimited teaching benefits ... effectively creating what they call "Classrooms of the Future".

"Teachers became comfortable with mobile technology, digital resources, and the advantages of every student having a computing device. They realized that classroom redesign and digital transformation has a big and positive impact on learning," said Sutorius.

It's no surprise that the initiative was a big success. The district is now a member of The League of Innovative Schools and hosts an annual Digital Conversion Symposium to help other districts navigate their digital transformation.

## Emotet slips past incumbent endpoint security

The IT team takes pride in following industry best practices in everything they do. "We adopt rigorous security controls and conduct regular penetration audits. This allows us to provide quality security and management for our systems," said Sutorius.

The team's best practices were put to the test when the invasive Emotet Trojan slipped past the district's incumbent endpoint security solution on the sixth day of school

"We started getting Help Desk calls that devices had blue screened, and quickly realized we had a significant issue," said Sutorius.

Emotet wasted no time. The Trojan spread laterally to other endpoints in the network. Within 24 hours, East Irondequoit had 1,400 infected computers.

> Malwarebytes made it possible to knock down the Emotet infection in twenty days without taking down our network. It's great to detect infections but to have a solution that also isolates and disinfects the infection is huge. I believe Malwarebytes has a powerful solution, and no one currently has anything close to it.
>
> Joseph Sutorius, Chief Information Officer
> East Irondequoit Central School District

## Malwarebytes to the rescue

The district IT team suspected that the incumbent endpoint security solution had let them down. After researching that vendor's knowledge base and other relevant online resources, they quickly decided they needed something more effective to detect and deal with the Emotet Trojan. Sutorius immediately pivoted on a mission to select an automated remediation tool to manage the incident response process.

His research lead him to Malwarebytes as the top selection. Sutorius also confirmed that it had positive reviews from Gartner Peer Insights, which helped validate that he had the right solution.

Sutorius started with Malwarebytes' free incidence response tool for expediency and then purchased Malwarebytes Endpoint Detection and Response (EDR) to automate and fully support the district's remediation.

Malwarebytes EDR was essential to the recovery efforts. The IT team installed the solution, and by mid-day, the central cloud-based dashboard provided the team critical insight to see the extent of the outbreak, which had reached nearly half of the network's machines.

"We marvel that Malwarebytes was nimble enough to help us out so quickly. We would have been in big trouble if we hadn't gotten the solution in place as fast as we did," said Sutorius.

## Automated remediation and Malwarebytes Nebula lead the way

Malwarebytes Nebula provided the command-central point for the team's remediation efforts. They accessed Nebula on their phones and on a browser from home to monitor progress. It provided a centralized view into which endpoints needed Malwarebytes EDR installed and allowed the team to identify new infections that were occurring via lateral movement.

"You can't put a price on the comfort level the Nebula platform gave my team to have eyes on the remediation progress. In contrast, our incumbent solution only showed us that we still had infections, and we had no insight if we were making progress. My team was doing their level best, and with Malwarebytes, they could quantify that their efforts were making a difference in remediating Emotet from the network," said Sutorius.

Nebula also enabled the team to identify machines that were getting re-infected. Sutorius called Malwarebytes Support to triage the issue. They realized Emotet had cracked the network's admin password, so it had access to deactivate endpoint security. Once the team addressed this issue, they made fast headway in removing all traces of Emotet from the network.

## Emotet knocked down in twenty days

Malwarebytes' automated remediation provided the powerful capabilities required to fully remediate Emotet from the district's network. The solution stopped web access on the devices, crippling Emotet's ability to obtain further command and control communication.

Malwarebytes EDR also isolated the endpoints, limiting communication only to the Nebula platform. This ensured the PC didn't get re-infected while Malwarebytes was removing Emotet and preserved the machine's clean state during the network remediation process.

"Malwarebytes made it possible to knock down the Emotet infection in twenty days without taking down our network. Without Malwarebytes, our remediation would have taken significantly longer and would have required a network interruption during our busiest time of the school year. We also received fantastic support from Malwarebytes during our remediation efforts," said Sutorius.

## Modern solution for the modern endpoint

The team's experience with Emotet and the support from Malwarebytes EDR have forever-changed their approach to endpoint security. Day-to-day, the team now vigilantly monitors for new infections. An employee opens the Nebula platform first thing in the morning and checks it throughout the day.

From a solution-perspective, Sutorius is a firm believer in having a modern endpoint security solution that has multiple protection layers and includes automated detection and response capabilities. "It's great to detect malware but to have a solution that also isolates and disinfects the infection is huge. I believe Malwarebytes has a powerful solution, and no one currently has anything close to it," said Sutorius.

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.