BULLWALL

CUSTOMER STORY

PROTECTING EDUCATION: HOW BULLWALL SAVED SIR ROGER MANWOOD'S SCHOOL FROM FOUR RANSOMWARE ATTACKS

Industry
Education

Location
United Kingdom

BullWall Champion
Sharn Somerton-Davies, IT Manager

600

Computers onsite during early Covid-19 lockdowns

17

Servers + multiple projectors, the telephone system and CCTV

1

User with remote access that bad actors used to bypass security measures

OVERVIEW

With a team of two looking after over 600 computers onsite, 17 servers, multiple projectors, the telephone system and CCTV, Sir Roger Manwood's School was a prime target for bad actors launching ransomware attacks. The attack came at 3.00am during the first national Covid-19 lockdown, and had a devastating effect. Bad actors had piggybacked on a user with remote access to launch their attack, bypassing preventative security measures and encrypting all files on the network. By the time IT staff got to the school the next morning, users were unable to log in.

> THE ATTACK CAME AT 3:00AM DURING THE FIRST NATIONAL COVID-19 LOCKDOWN, **AND HAD A DEVASTATING EFFECT.**

"When the attack occurred, we were fortunate that COVID-19 restrictions had already necessitated a lockdown and that it coincided with the school's half-term break" recalls Sir Roger Manwood's School IT manager, Sharn Somerton-Davies. "Google Classroom was already set up for students to work from home, which minimized disruption to their studies. However, our biggest challenge was the email system. With all servers down, users could not access or authenticate email accounts, effectively cutting off our primary means of communication."

PREVENTATIVE SECURITY DIDN'T WORK

With communications still down, relying only on an internal phone system and no email, and in the midst of a national lockdown, the race was on to get the school and its students back up and running. The IT team worked side by side to disconnect everything, clean the machines, and use available backups to recover lost files—a painstakingly slow process.

"The entire recovery process took about two weeks, during which time the IT team worked fourteen-hour days to assess, scan, and rebuild each system. Every machine on campus was reimaged to ensure no trace of the attack remained. The initial four days were dedicated to evaluating data integrity, assessing the servers we could operate without, and executing intensive cleaning processes on each machine. Communications during this time relied entirely on mobile phones, as our phone system had also been compromised. Meanwhile, our backup company meticulously analyzed data to trace the origin of the attack, which appeared to stem from a Remote Desktop Protocol (RDP) connection by one of our staff members."

The rebuild consisted of bringing every system and machine down to absolute minimal operating capacity with no internet connection, and then slowly and methodically working through what had been corrupted, where it had been corrupted, cleaning out any residuals and rebuilding from the ground up.

"As each server was reactivated, it was scanned, cleaned, and then taken offline again for another check. In total, we managed this process for 18 virtual servers. Alongside this, I made visits to staff members' homes to inspect and clean their laptops, installing new antivirus software to protect remote devices. We decided to ban all RDP access moving forward."

After ten days, the team were finally ready to reconnect the internet, but even then, email was cautiously held back as they went from workstation to workstation, scanning and monitoring each as it came online.

Communications during this time relied entirely on mobile phones, as our phone system had also been compromised. Meanwhile, our backup company meticulously analysed data to trace the origin of the attack, which appeared to stem from a ***Remote Desktop Protocol (RDP) connection by one of our staff members.***

Sharn Somerton-Davies
IT Manager,
Sir Roger Manwood's School

"Once email went live, the system was fully operational again. Despite Google Classroom allowing students to continue lessons remotely, the lack of reliable communication created immense pressure, and as the days passed, we faced constant questions and concerned looks from staff. Each step of the way was a reminder of just how critical secure, reliable systems are to the school's operations."

WORKING FROM HOME

With staff teaching from home because of the lockdown, it meant the IT team had to go on the road to clean and recover these machines. The process involved sitting outside homes and remote accessing their machines to make sure there were no residuals that could come back and affect the school again.

The detection of residuals was extremely difficult, and knowing what was corrupted was almost impossible, so when the time came to switch everything back on it was a tense moment.

Thankfully, the school was operational once again. However, as soon as this occurred, School Governors wanted to know what had happened and why. Their main question was, 'Could it happen again?' The only possible answer was 'yes.'

ANOTHER FIREWALL WON'T CUT IT

Within days of being back up and running, the IT team began to look for a solution. Business partners suggested additional firewalls; however, the team knew this wasn't the way forward. Fortunately, they discovered BullWall Ransomware Containment and knew immediately that they'd found their solution. After an initial demonstration followed by a ransomware assessment to show how the systems automation responds to attacks in real-time, the product was purchased and installed ready to take on the next attack.

Since installing BullWall the school has been attacked a further four times, and in each instance the attack has been thwarted by BullWall.

"We've had instances of packets being attached to what looked like legitimate HMRC Government emails going to the finance team, BullWall stopped that attack. We also received a PowerPoint file from a trusted source that was expected but again the ransomware had been embedded and would've quickly and easily spread if BullWall hadn't put an instant stop to it. Of the four attacks, three have been malicious and the fourth was a student who didn't have malicious intent, but had through their actions made us vulnerable. On all four occasions BullWall protected us."

SINCE INSTALLING BULLWALL THE SCHOOL HAS BEEN ATTACKED A FURTHER FOUR TIMES, AND IN EACH INSTANCE **THE ATTACK HAS BEEN THWARTED BY BULLWALL.**

I experienced an attack where a cybercriminal used a valid user account to get in remotely. You can't prevent that. ***You need a ransomware containment solution like BullWall.***"

Sharn Somerton-Davies

ABOUT BULLWALL

BullWall is the pioneer in ransomware resilience, providing robust defenses against the relentless threat of ransomware. Our focus on the latest ransomware tactics uniquely addresses critical gaps left by other security solutions. By delivering server-based protection without an endpoint agent, BullWall keeps critical IT infrastructure secure and operational during the core stages of an attack – before, during and after.

Learn more at www.bullwall.com.

BULLWALL