Overcoming The Attack

As Proton attempted to stabilize the network, they found locations within PCs and servers where hackers were still present. Proton had 120 PCs delivered overnight and quickly installed them throughout the dealership group so they could resume operations. Eventually, they would install 250 PCs total and add Remote Management Platform, Endpoint Detection and Response, and Security Event and Intrusion Management to the devices.

They had the dealership's firewall locked down and restored the backup servers. They rebuilt domain controllers and restored as much as they could.

What can you do to prevent this?

- Hackers typically don't hack machines, they hack people. Through Security Awareness Training, you can arm your personnel with the knowledge to recognize manipulation tactics used by hackers and stop an attempt before it ever starts.
- With Endpoint Detection and Response, your end-user devices will be continuously monitored to detect and respond to cyber threats like ransomware. Administrators can isolate a device to prevent an attack from spreading to the network.
- When network security issues are detected, Security Event and Intrusion Management can create alerts and instruct other security devices to mitigate the issue, ensuring malicious activity within your network does not go unnoticed.

These tools paired with Proton's Firewall Management and Backup & Disaster Recovery solutions provide dealerships with a high level of protection against these increasingly dangerous attacks.

For more information, visit **protontechs.com** or scan the **QR code.**

PROTON DEALERSHIP IT CYBER SECURITY | Reynolds & Reynolds®

The Timeline of a Modern Ransomware Attack

Dealerships have been faced with unprecedented levels of cyber attacks due to the amount of data collected each day. Ransomware, one of the most common attacks, is a form of malware that targets both human and technical weaknesses in an organization's network in an effort to block access to critical data and systems. These attacks encrypt networks and demand a ransom be paid, which can cost dealerships millions. The following is a real example of a ransomware attack at a dealership group that lasted five days and crippled most of the computers across their five dealerships.

Ransomware Detected

PROTON
DEALERSHIP IT
CYBER SECURITY

Ransomware Detected

Day 1

4:37 PM

The finance manager received a phishing email that seemed to be from the billing clerk. It used her name and a subject line from previous emails between the two. An attached Word document was opened and a macro was executed.

Prior to the attack, the billing clerk's email had been compromised by a platform called Emotet, which had been "secretly" capturing email data for 90 days.

Day 2

4:44 PM

Several trickbot modules were automatically downloaded and were instantly operating. They had already begun compromising the initial PC and entire network. They were looking for passwords, banking data, point-of-sale systems, etc.

Day 3

10:47 PM

Multiple network lateral movements were occurring, meaning a cybercriminal was hopping through networks looking for valuable data to encrypt and backups to destroy. Their goal was to execute maximum damage.

11:55 PM

Powershell Empire, an exploitation tool, was launched across the domain and most infrastructure was encrypted using the RYUK framework. Out of 29 servers, 25 were successfully encrypted.

Day 4

8:00 AM

Employees showed up to work and all computers either didn't work at all or had a "Ryuk" message on screen. The DMS didn't work so they could not service cars, write ROs, close deals, or execute any normal operations.

Day 5

Proton was contacted and began to regain control of the network. Over the next day and a half, the Proton team set up 120 PCs so the dealership could resume operations.