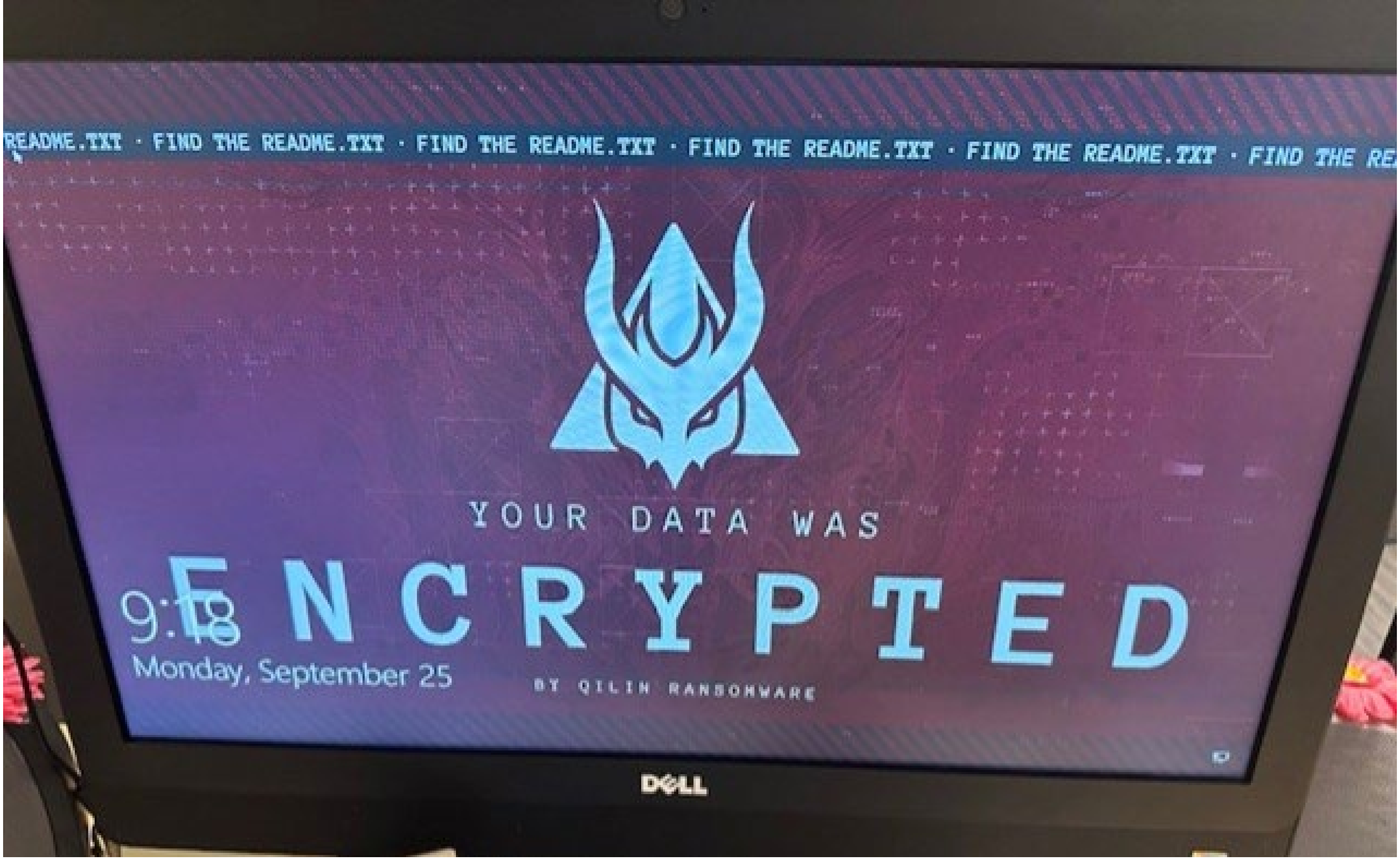
Surviving a Cyber Attack

Monday, September 24, 2023

Wednesday, December 16, 2024



README.TXT · FIND THE README.TXT · FIND THE README.TXT · FIND THE README.TXT · FIND THE README.TXT · FIND THE RE

YOUR DATA WAS

ENCRYPTED

BY QILIN RANSOMWARE

9:18

Monday, September 25

CUNY/Baruch College
20k students; 4K employees

Monday, September 24, 2023 (Yom Kippur)

-All Baruch servers affected (website, intranet, kiosks, payroll, ePAF, wordpress sites, email, VOIP phones, etc)

-All Baruch networked devices captured (desktops, laptops, lecture podiums, copiers, etc)

Pay us and we will give your servers back.

Response:

No ransoms paid.

Replace everything.

Yes, all servers, all hardware and devices.

Nothing from infected devices was recoverable.

Systems on local servers were rebuilt.

All remote with phased return to campus prioritizing classes. Last workers returned in December.

Graduate Suite Purview

PhD Payroll/Timesheets	Staff Timesheets	EPAF appointments	Endowed Scholarship	Student appeal materials	Curriculum committee program materials
Personnel files/guidance memos	Legacy admission database	Electronic Grading System/Approvals	Admissions files	Research material/Dedoose	Student Records
	Course Scheduling	Official curriculum/ bulletin	Admissions system	Research Foundation grant activities	

Heart of the Matter: Servers

- Dropbox
- Teams
- Campus Website/Instranet
- Campus Sharedrive
- OneDrive
- Blackboard/Brightspace
- Campus timesheet process
- Desktop
- Peoplesoft
- Slate/Hobsons
- Other local servers/not your campus

Take two: CUNY/Baruch College
20k students; 4K employees

On or about December 14, 2024

Finals period December 16-20.

-Attack detected

Little information shared on the nature of the attack.

Response:

All Baruch servers frozen/taken off-line for protection (website, intranet, kiosks, payroll, ePAF, wordpress sites, email, VOIP phones, etc)

Impact:

Finals room assignments not posted.

Finals that use technology/classroom podiums cannot be administered.

Delayed grade submissions.

Payroll repeated last run.

Some internal sites on servers were rolled back to before the attack- loss of content vital to process.

Right now

Back up your desktop to your local share drive. If you have extremely sensitive materials, work with IT to create a locked location.

Back up vital items into either print copies or to AWS server clouds, as your IT rules allow.

Make your IT folks at the institutional level aware of any local systems and any key dates of use. Develop these relationships, even a little.

Create a guide for new faculty, administrators, staff as to where things are saved and backed-up and why.

Create a training plan for any long-termers who may have ingrained habits. It hurts to loose 20+ years of files.