Control Cont	furction/contacted the standard for	name <imq>=s</imq>	ess logged ((if) no	etologiantola eta 2022/2014/2014/2014/2014/2014/2014/2014/	
Traction and the second of the	The state of the second second		a?:/c	(s) (logged = online.click) (ger.warning) #keu_input <chain> = (d fgi</chain>	_
For Common (and business and an accommon and a second and an accommon and accommon and accommon and accommon ac	madan C	еек			
script serve (true) local conf. (24, 23,86,878). Ransonware Attock of the house in the serve se	estate era often al local conflo	0.10		ess: status [true] :log.origin set (278,56,34,#)if = frame kir	-
script serve (true) local conf. (24, 23,86,789, true) for the property of the form of the property of the prop	man CUITO GIC	status, omm	ue') add.st	Key_inpub-	
Tock.command # onecosis denail // text text tock.command # onecosis denail // text text tock.command # onecosis denail // text text tock.command # onecosis denail // text tock.command # onecosis denail // text tock.command # one one of text tock.command # one one one one of text tock.command # one one one of text tock.command # one one of text tock.command # one one of text tock.command # on	script src=[true]local.confi logged:#Input false fun	(245, 23, 068, 789, n name < img> = spa	ress logged < [if] n	OQ. OF INTEREST AND A STATE OF THE PARTY OF	-
"Simution lagged amout faither function lagged a only sc n) boat coming status and referred for several resolution and several representations of the several resolution and several representations are several representations and representations are several representations and representations are several representations are several representations and representations are several representations and representations are several representations and representations are several representations.	<pre>// script src= address [lock.command]#>>access:denial //</pre>	atus?] code<[tr t src=[erro c	tus (m#4:80a?: de logged {t	(logged was restrict.) F. war nine for the longer state of the second	
Rection appearance fels to unbrance and wino . (tru onf sc (?u nown) local config status error e	function logged: # input false function logged: #	onfig so		n) local config status - Proh(error)	_
	Apotter appearance felt for the house of a temperature of a temperature of the second	np .[tru onf so	(?u n	own) local.config status = error (error)	

Indian
Creek
Foundation

- Nonprofit Behavior Health Agency in Souderton PA
- 1750 Clients
- Three Primary Programs

 - Residential adultsDay Services adultsBHS

 - Outpatient Clinic adults and children
 IBHS children
 Afterschool and Summer Camp children

Charles Lockett clockett@indcreek.org

- Application Software Design and Development
 Database Design
 Project Management
 Workflow Analysis

Infrastructure and Application Landscape

- 300 Users
- 5 Internal Servers, 150 desktop PCs, 30 laptops
- 8 Highspeed Printer/copier/scanners
- Facility Security cameras, door access
- Time and Attendance system Self Hosted
- GL and AP Accounting systems Self Hosted
- Residential Staff Scheduling system Self Hosted
- EHR system Cloud Based
- Microsoft Office 365 Cloud Based
- Payroll Cloud Based

The Attack

- Discovered February 6th by IT Support Staff
- Appeared to be a network failure
- Unable to sign on to the primary network console
- Unable to sign on to any PC attached to the network
- Ransomware message, with instructions, was displayed on an alternate network console
- Was later learned that the hackers gained access through a dated remote access utility and spent 6 hours roaming through the network

The Damage

- All files on the network servers were encrypted
- All files on the network connected PCs were encrypted
- All file extensions were changed to "LOCKBIT"
- Time and Attendance system was disabled
- Accounting systems were disabled
- User PCs were disabled
- Shared drives were not accessible
- Printers/copiers were disabled
- Time clocks were disabled
- Building security systems were disabled

Mitigation Plan	Limit client and service disruption Contact insurance carrier Crisis Team assigned - Specialized Law firm and a Forensic data group No contact with threat actor Shutdown network (and all remote access) Continue to work remotely (Cloud based applications only) Manual time sheets Restore backups Move accounting systems to a local network	
		1
Remediation Plan	Forensic analysis How was access gained and secure it, was data taken? No ransom paid Restore/Replace effected PCs Third party assistance Engaged third party network support Monitor network, active virus detection and backups Move self hosted applications to the cloud Time and Attendance and Accounting systems Engage third party Data Mining group Employee and Client data was exposed Breach notifications (State and HIPPA)	
		1
Thank You	Questions, Comments?	