Show description

Rigel Cybernetics Institute Case File

Timeline | Threads (Overview) | Emails (by Day) | Emails (by Thread)

Day 1 (Friday) 19

Name	Thread	Chain S...	Subject	From	To	Email body	Attachments	Day	Date
Email 1.1	IT chain 1	1	URGENT!! Cannot access patient records	Sosy Kovács (skovacs@intake.rigelcyberinstitute.com)	IT (it@rigelcyberinstitute.com)	VERY URGENT REQUEST! Everybody on my floor is reporting the patient record server isn't responding anymore. Same situation on Floor 4 too. Can somebody fix it ASAP? We're running blind right now - nobody can pull up any records Sosy Kovács Front Desk (Floor 3) Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 6:33
Email 1.2	IT chain 1	2	RE: URGENT!! Cannot access patient records	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Sosy Kovács (skovacs@intake.rigelcyberi...	Thank Sosy. Just sent Avery down to take a look at the EHR system. Will keep you posted. ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 6:41
Email 2.1	IT chain 2	1	EHR-14 patient records server status	Avery Shapiro (ashapiro@it.rigelcyberinstitute.com)	Shanice Campbell (scampbell@it.rigelcyb...	Hey Shanice. Sooo the server is showing this ransom note. (See attached.) Guessing that's the problem. ...I'm afraid to ask. When's the latest backup of the EHR-14 server? Avery S. IT Services Rigel Cybernetic Institute	Email 2.1 - WannaCry ransomware note.png	Day 1 (Friday)	2024/11/01 6:56
Email 2.2	IT chain 2	2	RE: EHR-14 patient records server status	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Avery Shapiro (ashapiro@intake.rigelcyb...	Holy what the... How the HECK did our patient records server get hit with WannaCry? (...please tell me you're trolling.) ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 6:58
Email 2.3	IT chain 2	3	RE: EHR-14 patient records server status	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Avery Shapiro (ashapiro@intake.rigelcyb...	Our CMDB doesn't even list EHR-14, much less the software it was running. Or any backups (anywhere?). Are you sure this is the right info? ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 7:04
Email 2.4	IT chain 2	4	RE: EHR-14 patient records server status	Avery Shapiro (ashapiro@it.rigelcyberinstitute.com)	Shanice Campbell (scampbell@it.rigelcyb...	Yeah...I'm sure. There's a physical label that says "EHR-14" on the device, and when I look in Wireshark, all the workstations are trying to connect to ehr-14.rigelcyberinstitute.local. EHR-14 is definitely the patient records server. And it is definitely infected with WannaCry. p.s. Kinda wishing we'd made tuning the SIEM a higher priority...right around...now... Avery S. IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 7:05
Email 1.3	IT chain 1	3	RE: URGENT!! Cannot access patient records	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Sosy Kovács (skovacs@intake.rigelcyberi...	Hi Sosy. Bad news. The patient data server is going to be offline for the foreseeable future. It has been encrypted with ransomware. We're sending Bob and Alice down to assist. ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 7:07
Email 1.4	IT chain 1	4	RE: URGENT!! Cannot access patient records	Sosy Kovács (skovacs@intake.rigelcyberinstitute.com)	Shanice Campbell (scampbell@it.rigelcyb...	Are you serious?!!! How could you have let this happen! I need to go focus on doing my job. And maybe you should focus on doing YOURS, too, considering preventing THIS from happening isn't part of MY job responsibility. Sosy Kovács Front Desk (Floor 3)		Day 1 (Friday)	2024/11/01 7:09

Day 1 (Friday) 19

Name	Thread	Chain S...	Subject	From	To	Email body	Attachments	Day	Date
Email 2.5	IT chain 2	5	RE: EHR-14 patient records server status	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Avery Shapiro (ashapiro@intake.rigelcyb...	...there goes our weekend. I'm looking for our IRP. Didn't Sean update it last year? ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 7:17
Email 2.6	IT chain 2	6	RE: EHR-14 patient records server status	Avery Shapiro (ashapiro@it.rigelcyberinstitute.com)	Shanice Campbell (scampbell@it.rigelcyb...	Yeah, I think it's in the old Google Drive. Avery S. IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 7:36
Email 2.7	IT chain 2	7	RE: EHR-14 patient records server status	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Avery Shapiro (ashapiro@intake.rigelcyb...	K, I'll look there. The only copy of an IRP I can find is from five years ago, before we acquired the hospital campus. (Pretty useless.) I've sent Bob and Alice down to the floor to help Sosy etc try to manage the staff without the server. Huston is now in the server room looking for a backup for EHR-14. Hopefully somebody made one and just forgot to document it since the device isn't properly recorded in iTop 🤞 LMK as soon as you find Sean's IRP rev ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 7:54
Email 3.1	IT chain 3	1	EHR-14 backup status	Huston Kurosawa (hkurosawa@it.rigelcyberinstitute.c...	Shanice Campbell (scampbell@it.rigelcyb...	Hey Shani, **Good news:** there's a backup! **Bad news:** the backup is eight months old. Huston K. IT Services		Day 1 (Friday)	2024/11/01 10:12
Email 3.2	IT chain 3	2	RE: EHR-14 backup status	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Huston Kurosawa (hkurosawa@it.rigelcyb...	Well. That...is not ideal. I guess we're going to have to pay the ransom, then. ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 10:15
Email 4.1dax	IT - CEO - CTO	1	We need to pay the ransom	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Willa Herzog (herzog@rigelcyberinstitute... Gregory Saragossa (saragossa@rigelcyb... Anaïs Belleview (anais@rigelcyberinstitut...	UPDATE: Looks like we'll need to pay it. The latest backup of the patient records is eight months old. We will need to pay the ransom to get operations functional ASAP. Do we need to notify the FBI or can we just go ahead? ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 10:15
Email 4.2	IT - CEO - CTO	2	RE: We need to pay the ransom	Willa Herzog (herzog@rigelcyberinstitute.com)	Gregory Saragossa (saragossa@rigelcyb... Anaïs Belleview (anais@rigelcyberinstitut... Shanice Campbell (scampbell@it.rigelcyb...	Alex & Shanice: I'm authorizing the transmission of funds to pay the ransom. We're losing money by the minute. We've already had to negotiate moving a few critical patients to another facility. Let's get this done ASAP. Willa Herzog CEO Rigel Cybernetics Institute		Day 1 (Friday)	2024/11/01 10:28
Email 4.3	IT - CEO - CTO	3	RE: We need to pay the ransom	Anaïs Belleview (anais@rigelcyberinstitute.com)	Willa Herzog (herzog@rigelcyberinstitute... Gregory Saragossa (saragossa@rigelcyb... Shanice Campbell (scampbell@it.rigelcyb...	All right. I'm going to authorize the transmission of the funds into a crypto wallet. Shani, can you handle paying it once there? I don't think we need to notify anybody. Anaïs Belleview Chief Financial Officer Rigel Cybernetics Institute		Day 1 (Friday)	2024/11/01 10:33
Email 4.4	IT - CEO - CTO	4	RE: We need to pay the ransom	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Willa Herzog (herzog@rigelcyberinstitute... Gregory Saragossa (saragossa@rigelcyb... Anaïs Belleview (anais@rigelcyberinstitut...	Handling it now. Will update once the server is decrypted. ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 10:43
Email 4.5	IT - CEO - CTO	5	RE: We need to pay the ransom	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Willa Herzog (herzog@rigelcyberinstitute... Gregory Saragossa (saragossa@rigelcyb...	Very bad news: the decryption key provided is broken. The server can't be decrypted even though we've paid the ransom.		Day 1 (Friday)	2024/11/01 11:37

Day 1 (Friday) 19

Name	Thread	Chain S...	Subject	From	To	Email body	Attachments	Day	Date
Email 4.5	IT - CEO - CTO	5	RE: We need to pay the ransom	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Willa Herzog (herzog@rigelcyberinstitute... Gregory Saragossa (saragossa@rigelcyb... Anaïs Belleview (anais@rigelcyberinstitut...	Very bad news: the decryption key provided is broken. The server can't be decrypted even though we've paid the ransom. We'll need to rely on the eight-month old backup. ~Shanice IT Services Rigel Cybernetic Institute		Day 1 (Friday)	2024/11/01 11:37
Email 4.6	IT - CEO - CTO	6	RE: We need to pay the ransom	Willa Herzog (herzog@rigelcyberinstitute.com)	Gregory Saragossa (saragossa@rigelcyb... Anaïs Belleview (anais@rigelcyberinstitut... Shanice Campbell (scampbell@it.rigelcyb...	Greg, Anaïs, Shani: We all need to have a meeting. Now. Meet me in the conference room on the 5th floor. I'll be there in 5 minutes. I expect you all to be there by the time I arrive. Willa Herzog CEO Rigel Cybernetics Institute		Day 1 (Friday)	2024/11/01 11:41

Day 2 (Saturday) 4

Name	Thread	Chain S...	Subject	From	To	Email body	Attachments	Day	Date
Email 2.8	IT chain 2	8	RE: EHR-14 patient records server status	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Avery Shapiro (ashapiro@intake.rigelcyb...	Finally found the IRP. (Better late than never, I guess?) Apparently Sean updated it *two* years ago. (yikes) ~Shanice IT Services Rigel Cybernetic Institute		Day 2 (Saturday)	2024/11/02 12:24
Email 2.9	IT chain 2	9	RE: EHR-14 patient records server status	Avery Shapiro (ashapiro@it.rigelcyberinstitute.com)	Shanice Campbell (scampbell@it.rigelcyb...	Oof. This document is useless. It's mostly placeholders. Avery S. IT Services Rigel Cybernetic Institute		Day 2 (Saturday)	2024/11/02 12:47
Email 2.10	IT chain 2	10	RE: EHR-14 patient records server status	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Avery Shapiro (ashapiro@intake.rigelcyb...	Well...as I recall, Sean was going through a tough time personally at the time. *I* should've noticed this when I took over his role months ago. This is my fault. 🤦‍♀️ ~Shanice IT Services Rigel Cybernetic Institute		Day 2 (Saturday)	2024/11/02 12:59
Email 2.11	IT chain 2	11	RE: EHR-14 patient records server status	Avery Shapiro (ashapiro@it.rigelcyberinstitute.com)	Shanice Campbell (scampbell@it.rigelcyb...	You had so much on your plate — I'm not surprised this fell between the cracks, between the migration to the new IP phone system and the new vendors we had to integrate as soon as you started that role... I just wish we'd tested this beforehand with a tabletop. Would've noticed all the placeholders then. :/ Avery S. IT Services Rigel Cybernetic Institute		Day 2 (Saturday)	2024/11/02 13:02

Day 3 (Sunday) 8

Name	Thread	Chain S...	Subject	From	To	Email body	Attachments	Day	Date
Email 5.1	CEO - CTO 1	1	Investors need answers	Willa Herzog (herzog@rigelcyberinstitute.com)	Gregory Saragossa (saragossa@rigelcyb...	Greg: Investors need answers. How on earth did we not have our assets properly protected AND backed up? This incident is costing us thousands of dollars in lost revenue each day. (Don't even get me started on the damage to our reputation and customer trust!) When was our last audit? How did any of this happen? Don't we have security monitoring set up to detect this stuff BEFORE it impacts our bottom line? I thought it was VERY clear what our business priorities here at Rigel are: - exceptional patient care - innovative software development for delivering that exceptional patient care - impeccable protection of customer privacy How did this fall between the cracks? Willa Herzog CEO Rigel Cybernetics Institute		Day 3 (Sunday)	2024/11/03 9:32

▼ Day 3 (Sunday) 8

Aa Name	Thread	# Chain S...	Subject	From	To	Email body	Attachments	Day	Date
Email 5.2	CEO - CTO 1	2	RE: Investors need answers	Gregory Saragossa (saragossa@rigelcyberinstitute.com	Willa Herzog (herzog@rigelcyberinstitute...	Hi Willa. Great questions! I'll need to get back to you about that. —Greg.		Day 3 (Sunday)	2024/11/03 10:04
Email 6.1	IT chain 4	1	How did they get in?	Gregory Saragossa (saragossa@rigelcyberinstitute.com	IT (it@rigelcyberinstitute.com)	Team, Do we have any idea how this happened? We need to find out. Fast. —Greg		Day 3 (Sunday)	2024/11/03 12:37
Email 6.2	IT chain 4	2	RE: How did they get in?	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Gregory Saragossa (saragossa@rigelcyb...	Hi Greg. I've spent the past day going through logs. Turns out a bunch weren't being parsed correctly, so the alerts we'd set up didn't fire. For instance: - Looking more closely at the logs coming in from snort-sensor-2 (192.168.1.219), I see a Snort alert for unusual egress traffic last Tuesday night. (Possible data exfil event?) - There's also several bouts of scanning activity originating from Records-013 going back to the end of September (!!). - Our last authorized audit was in August, so digging into the (until now, unexamined) Snort logs associated with that workstation showed consistent C2 traffic associated with a Meterpreter implant. - We see consistent traffic between Records-013 and EHR-14 during the same time period as the C2 Snort alerts. - We see evidence of ARP spoofing to intercept LAN traffic during this time period as well. We are still figuring out which attachment she (Records-013 user = Asma Zarif) opened. - Running hypothesis: The attacker probably sent her some bogus patient records and that's how her workstation got infected. - We've pulled the workstation for forensic examination to identify the malicious attachment. ~Shanice IT Services Rigel Cybernetic Institute		Day 3 (Sunday)	2024/11/03 15:12
Email 6.3	IT chain 4	3	RE: How did they get in? (UPDATE)	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Gregory Saragossa (saragossa@rigelcyb...	So. I have bad news. I did some investigating after seeing that possible data exfil event, and...uh. The attackers appear to be selling the data they stole from our server on an underground forum. Data sample appears to be legitimately ours (except, unlike our 8-month old backup...their sample appears to be from...last Tuesday.) ~Shanice IT Services Rigel Cybernetic Institute		Day 3 (Sunday)	2024/11/04 5:43
Email 6.4	IT chain 4	4	RE: How did they get in? (UPDATE)	Gregory Saragossa (saragossa@rigelcyberinstitute.com	Shanice Campbell (scampbell@it.rigelcyb...	...no. You can't be serious. —Greg		Day 3 (Sunday)	2024/11/04 7:27
Email 6.5	IT chain 4	5	RE: How did they get in? (UPDATE)	Shanice Campbell (scampbell@it.rigelcyberinstitute.c...	Gregory Saragossa (saragossa@rigelcyb...	Dead serious. We need to report this data breach. And our IRP only has placeholders for the section on where to report any breaches of consumer data. On the brighter side of things, this means we COULD purchase the up-to-date database that we could not decrypt with that broken decrypter... ~Shanice IT Services Rigel Cybernetic Institute		Day 3 (Sunday)	2024/11/04 8:09
Email 6.6	IT chain 4	6	RE: How did they get in? (UPDATE)	Gregory Saragossa (saragossa@rigelcyberinstitute.com	Shanice Campbell (scampbell@it.rigelcyb...	Meet me at Willa's office. Now. —Greg		Day 3 (Sunday)	2024/11/04 8:14

▼ No Day 2

Aa Name	Thread	# Chain S...	Subject	From	To	Email body	Attachments	Day	Date
	IT chain 2								2024/11/02 18:30 → 21:30
	IT chain 4								2024/11/04 9:00 → 12:00