How The 9R1nC4 0wned Xmas[1]

An attack analysis by Paul Hosking

Everyone who's who in Bedford Falls liked it a lot...
But Potter, who lived in an estate north of town, did NOT!
Potter hated them all and greed was his reason.
"Without those chumps undercutting business, I would make out this Christmas season!"
He schemed a scheme to bring Bedford Falls to its knees!
Why he would clear away all those whos and dogooders and do what he pleased!
The news this year exclaimed "SCADA security is weak!"
So Potter hired himself a hacker who was rumored to have deft technique.
The hacker went by the handle of the "9R1nC4" claiming no moral qualms,
He would pwn any newbs if enough Bitcoins crossed his palms.
The 9R1nC4 started his gig with a bit of reconnaissance...
Gathering employee names, equipment makes, and even network documents.
And so he knew what he knew to know he was on track,
When he crafted a carefully composed email phishing attack. [2]
For he knew the target had a Simatic S7-1200 PLC. He knew its IP.
He knew that unpatched, that kit had a cross-site scripting vulnerability.
He crafted a crafty URL that would connect to his own server for a stealthy trip.
The URL would dial home and embed his own devised java script!
But he didn't know for sure whether the phishing email hit Don Sawyer's inbox.
And he didn't know that Don Sawyer ran NoScript on Firefox.
So when Don haplessly moused over the confusing url quick,
And dutifully followed the instructions with a click,
That NoScript parsed the maliciously crafted URL as emailed,
And rendered a harmlessly filtered version so the attack silently failed.
But the 9R1nC4 wasn't done - oh but he was just warming up to the fight!
Next he dressed up business-casual and drove over to visit the site. [3]
He strode through the Valley Electric Company lobby with a confident air.
He strode down the hallways as if he had every right to be there.
He strolled purposely until he found a wiring closet,
He dodged through the door as quick as a rocket.
Inside he found the network gear he had sought...
"Let's see," he pondered as he read "Traffic Net" and "Ultility Net" "Now... which port?"
From his pack he pulled two wall-warts - Thing One and Thing Two.
He plugged in ethernet links on one side and then plugged them in to the PDU.
He zipped up his pack, pleased with his work and ready to prowl,
When he heard a sudden noise like the hoot of an owl!
"Who are you?! And what are you doing in here?"
Demanded a voice surprisingly near.
The 9R1nC4 turned around fast to see...
Cindy Lu who was the receptionist - not someone from IT.
"Why I'm the network consultant on call," he slickly lied.
"There's a router here that won't light up on one side."
He produced a professional business card with flippity-flup,
"You can call my case manager - he'll clear it all up."
But every call made gave Cindy Lu a busy tone,
Until the 9R1nC4 finally said "tell him we have to reschedule when you get him on the phone."
And so soon the 9R1nC4 was across the street at the coffee shop,
Hacking at wifi range and enjoying his risk-free coffee - every drop.

He connected to Thing One and wasted no time at all,
He fired off an ARP ping and then port scanned for common industrial protocol.
The port scan returned its findings with a list of hosts and little fuss.
And the protocol every host wanted to hear was for the industrial control Modbus.
The 9R1nC4 declared “now this is something I would like to see!”
He knew it would be possible - as simple as A R P.
A bit of ARP poisoning would set him up in a man-in-the-middle way.
He told Host A that his MAC was for Host B and Host B that he was Host A. [4]
And for each set of ARP announcements, he backed it up with another lie,
He crafted matching set of MAC-spoofed ICMP echo request and echo reply.
In no time at all, he found himself in a monkey-in-the-middle game.
Traffic came to him From Host A for B which he passed to B as if A and he were the same. [5]
He observed the Modbus traffic from Master to Slave and back,
Until he was quite sure of the patterns and ready to give it a whack.
He reversed all targeted ARP tables with gratuitous ARP announcement fanfare.
It didn’t completely work as some hosts didn’t accept the new ARP update... but he didn’t care.
The 9R1nC4 had already moved on to downloading a modbus scanner and a packet crafter.
He would take what he learned and totally pwn this network! He could barely contain his laughter.
The scanner scanned and he crafted modbus commands,
But everything returned errors; he didn’t quite understand.
“If you can ping it, you can own it” was the mantra for this stateless, ancient protocol.
But it wasn’t going that way - no, not at all. Maybe they had an application firewall? [6]
The 9R1nC4 was bored... bored, bored, bored with this Modbus rigamarole.
“Enough of this,” he grumbled, “I think I’ll look into that online water facility control.”
He hit the control application with his MacOS box via HTTP,
Without SSL, we was able to hijack a session just to see what “Operator” could see.
What he found thrilled him even more than the developer’s failure to encrypt,
A key piece of the application was a report generating PHP script.
“Why what do we have here,” he said with a smirk on his face, “I bet this application talks to a SQL database!”
And he loaded up sqlmap to see if that was, indeed, the case.
Oh but it was! And what brought the 9R1nC4 delight as sqlmap ran its inspection,
Was that the PHP script was totally susceptible to SQL injection.
The sqlmap mapped out the database, ANDing and SELECTing, it did its thing,
But the best was OUTFILE to /var/www/tmpurykq.php dumping a translated long hex string.
The 9R1nC4 did HTTP GET tmpurykq.php from the server’s web root folder,
Executing an application he had just written to the server called “sqlmap file uploader.”
Using the new script, the next order of business at hand,
Was to upload yet another a script that would execute any given shell command.
With access to a shell, and verification of functionality, next was a ‘ls’ of the directory
Just to see if there were other scripts right there to see.
And there were more PHP scripts - now this had potential!
He grepped them for “mysql_connect” and found database credentials!
“Now for some mysql commands using this webapp account!”
The 9R1nC4 modified the measurement_level for fluoride to a “0” minimal amount.
“That seemed to go well,” he thought with added glee.

Next came the command to additives table to zero and make fluoride an absentee.
But the response filled the 9R1nC4 with rage!
Right there displayed “command denied to user” - right there on the page!
“Oh what the frick!” growled the 9R1nC4 in sour disposition.
“Who the heck runs a webapp with limited database permissions?!”
Now this was annoying. Denied a quick collection of his fee.
Denied three times by this, checking the employee roster, George Bailey, CISSP.
The next day found the 9R1nC4 in a better mood,
As he took position in the coffee shop with a quad-shot latte and a bit of food.
“Let’s see what there is on this other network to do.”
As he picked up the signal and logged in to Thing Two.
He started off the session like he did with Thing One,
An ARP ping and a SYN scan for the entire 8-bit subnet run.
And just for giggle, he gave another try to the ‘ole ARP poisoning trick.
But either router or hosts would have none of it and none of his bogus ARP messages would stick.
“Well seems this network is a bit better protected,”
The 9R1nC4 had to admit feeling a little bit dejected.
Next came the standard flurry of packets hitting sockets on each industrial protocol port,
Generating a rather succinct list of open services to the report.
He pointed his browser at yet another web front-end for the Rockwell Automation vendor,
Thoughtfully pondering the output his browser did render.
“Why a MicroLogix 1100 Processor,” the 9R1nC4 muttered, his attention was engrossed.
“I seem to remember an interesting bit on a PLC users forum post.”
He snapped to attention with no time to waste,
He threw the mrplc.com URL at wget to snag the post... post-haste.
“Factory default credentials are a haxor’s best friend!”
The 9R1nC4 entered the provided credentials in to the MicroLogix’s web front-end.
“Denied” was the response to the attempted log-in, but the 9R1nC4 took it in stride.
“I guess factory default passwords was too much to expect,” he sighed.
The 9R1nC4 took some time off to consider his strategy.
(He lost most of the day when he Google-wandered in to XKCD.)
Back on track again, he came to mind this George Bailey, CISSP.
For every technical weakness he considered a guaranteed breach,
Each one of them; “low hanging fruit” plucked out of reach.
There has to be something! This armor must have a chink!
There had to be a way to attack this hardened target - he just had to think!
For as he thought and he thought about security configuration,
It dawned on him one morning that he misread the situation!
He knew the weakness - he suddenly saw the light.
The thinking and setting up the next attack took him almost a fortnight.
“There’s always more phish in the sea!,”
Snickered the 9R1nC4 as he crafted another email ever so craftily.
“Why poor George - he needs help with his task!”
“Surely George could rely on a fellow employee - all he need do is ask!”
The email from “George” asked Don Sawyer to download an executable binary. But of course,
Don wouldn’t be foolish enough to do so from an external source.
And this is where the 9R1nC4 had himself a little fun,
For the domain name slyly replace the “i” in “electric” with a “1”. [7]

So when Don clicked and began his download for an “internal” site’s file,
The bits came from a fully qualified domain name that the 9R1nC4 had registered for awhile.
The bulk of the binary Don haplessly executed dutifully,
Was no more than the benign Apache Bench benchmarking utility.
But piggyback to the normal app was a trojan that was also run,
Which contained a meterpreter proxy that dialed home to Thing One.
It was quite late on Christmas eve so the 9R1nC4 took position in his car,
In the same parking lot as the coffee shop’s strip mall - excellent wifi signal and not too far.
A sip of his hot coffee as he logged in to Thing One, sniggering with elation,
He could now proxy all his metasploit traffic through Don Sawyer’s workstation.
He got down to business, did a quick little scan to see what he could see.
It didn’t take long to find another server there talking SMB.
He pointed metasploit at this new host using the smb_login scanner,
He plugged in a user-password file he hacked together - letting it run in a brute-force manner.
The 9R1nC4 wasn’t confident he would see success with repetitive authentication braun,
He’d probably lock out accounts quickly... but he let it bang against “ernie” on and on... and on.
And to his surprise, there he was with success!
He had a brute force login - a local admin, no less!
He switched the meterpreter interface to pfexec, flingers flinging across the keyboard surface.
Metasploit built a payload, uploaded it, and executed it on the target as a service. [8]
Oh how the 9R1nC4 had Thing One already banging at his victim for VNC,
So when the GUI came up, he began to chuckle oh so darkly.
Oh what joy! What pwnage! The times for Bedford Falls were indeed quite dour!
Here in his VNC session, was the control for the town’s power!
The 9R1nC4 allowed himself to savor the moment before he dove for the jugular lickity-split,
And he cut generator power... he cut it off with a clickity-click.
Then he did one last thing, just to turn a few screws,
He launched Wordpad and typed “Merry Christmas, George Bailey! You lose!”
“Boohoo for Bedford falls!” he was ironically humming.
“They have no power - and with Christmas day coming!”
"They're just realizing it! I know just what they'll do!"
"Their mouths will hang open a minute or two,
Then they’ll look for someone to blame, that’s just what they’ll do!"

"That's something," grinned the 9R1nC4, "That I simply MUST see!"
“The lynching of George Bailey, CISSP!”
So he locked up his car, and walked down Main Street.
Nodding to people he didn’t know; every one a stranger he did meet.
But the anger didn’t come. People simply blinked against the dark.
They played in the snow. Christmas was here. It was all a grand lark!
It didn’t take long for the power to come back once the controller was checked.
And the 9R1nC4 realized that his efforts would have no lasting effect.
And he puzzled this for a few hours, his bruised ego a little sore.
Then the 9R1nC4 thought of something he hadn't before!
“Maybe all this,” the thought, “has greater worth than what you can get in a store.”

“Maybe all of this... maybe... means a little bit more...?”
And what happened then? Well - on the ‘Net they say,
The security posture of Bedford Falls’ utilities improved in six ways that day!
The 9R1nC4 wrote a final email to try and make amends.
He included advice that would have foiled his attempts, though it would make no friends.
“Well you dudes might want to start with a simple Domain lockout policy.
Then maybe consider a web content proxy.”
“I mean seriously,” the email went on, ”these are control stations not your home entertainment.”
“And speaking of which, a bit better network segregation with strong border containment!”
“And all those web front-ends and applications? Good certs and only HTTPS connections!”
And then the 9R1nC4 pondered - giving it further reflection.
“You’ll find a couple rogue access points in your wire closet - they’re wireless!”
“Oh. And I totally pwned you guys with trojans. Next time even the control workstations get anti-virus.”
“And one last thing to work on,” the 9R1nC4 wrote as he thought it worth a passing mention,
“You might want to scrub your email stream a bit better and give phishing some attention.”
And as he sent his email, the 9R1nC4 thought to himself “well - that’s that.”
And he, he himself! The 9R1nC4! He uninstalled the RAT.

---

[1] Or... One Holiday Classic Spoof Deserves Another
[2] With hasborg.com in the Message-Id no the less!
[3] The pcap doesn't actually demonstrate this but it explains where some attack hosts come from. And I claim creative license! It fits with the story theme.
[4] There are, of course, more than 2 (or 3) hosts involved. But our attacker ARP poisons hosts in pairs, corrupting each host's ARP table entry for the other.
I didn't want to break up the meter of the story by getting in to details. On reflection - rhyme is a poor agent to deliver attack analysis.
[5] Spoofing MAC addresses accordingly, of course.
[6] So why didn't he go back to spoofing traffic and inject his own commands? I'm guessing it's because he was using Ettercap for ARP poisoning and didn't have a proper utility to inject Modbus commands.
[7] This trick actually appears in both phishing emails - it is the domain our attacker is using for his from address. But it is being used to different effect here.
[8] The attack payload file was PjzJEubs.exe - but not that important as it’s automagically generated by Metasploit. Doesn’t trip many AV either.