Twitter Thread by Jake Williams



Jake Williams
@MalwareJake

Twas the night before Christmas and all over the ‘net,
Not a creature was stirring except a few cyber threats
The firewalls were configured at the egress with care,
But that wouldn’t stop us from being hit by ransomware. 1/

The children were nestled all snug in their beds,
While attackers hit the web server and established a beachhead
Mama with her EDR and I with my IDS
Were ready to tackle this hot infosec mess. /2

Down in the SOC there arose such a clatter,
I logged into my dashboard to see what was the matter.
This thing had better work, it cost so much cash.
How in 2020 can this thing STILL require Flash?! 3/

The alerts lit up the dashboard, it produced such a glow
But it’s because the threshold for alerting was configured so low.
When what to my wondering eyes did appear,
But 300 false positive alarms. I thought “I’ll be here all year.” 4/

Then a little old DLL, signed by SolarWinds,
Was really the Russians, masters of supply chain break-ins.
We need some new vendors said the CISO, and the salespeople came. 5/

She shrugged, and she grunted, and she called them by name:
Now AlertDashboard, Now FaceDancer, Now PacketPrancer, and CyberOxen.
On DarkComet, On WebCupid, On DataDumpDonner, and BlinkenBoxen! 6/

With no DNS filtering and egress that was open to all,
The Russians said “why even bother to deploy a firewall!
The off-site DFIR team prepared here to fly,
But with no logging configured, things were going awry. 7/

Their OPSEC was bad and the attackers they knew,
So their rootkit crashed a critical server with a death screen of blue.
“It might not be Russia, the packets could be a spoof!”
“But attribution is nuanced, and you’ll never have proof” 8/

The analyst checked the logs, and then spun around,
Saying “there’s nothing we missed, supply chain attacks are profound”
The CEO was worried Russians wanted his secrets to loot,
But the CISO said “we told you that’s China, you’re not being astute.” 9/

A cluster of servers, secured in their locking rack,
Still fell victim to this insidious cyberattack.
The alarms on the dashboard – oh how they twinkled! This one’s gonna be hairy…
The CISO admitted “this one is bad, I’ve never seen malware so scary!” 10/

The boss said “get this incident done, wrapped up with a bow”
But the CISO said “this isn’t CSI:Cyber, it’s going to be slow”
The boss said “this was preventable but your skills are beneath”
The CISO responded “stop insulting my team or I’ll knock out your teeth” 11/

The CISO ruled with an iron fist, just like Machiavelli,
And said “follow the 3-2-1 rule so we aren’t all so smelly!”
The budget was plump, a sign of cybersecurity health,
Everything purchased had been installed – nothing bit-rotting on the shelf. 12/

A wink of her eye and a twist of her head,
Soon gave me to know infosec misogynists would be dead.
“Why?!” said the analyst, “we’re just having fun at work!”
She said “Stop being a Neanderthal, a dope, and a jerk!” 13/

As every incident responder most certainly knows,
Working incidents through the holidays absolutely blows
The IR team remediated the issue and one of them let out a whistle.
The team lead said “if you leak to the press, expect a dismissal.” 14/

Then I heard them exclaim as they drove out of sight – “Just stop clicking on stuff, we can’t do this again tonight!”

Happy whatever you celebrate from all of us at @RenditionSec to you and yours! /FIN

https://t.co/tdwkMSseJc

> If you prefer the recorded version, here it is too.https://t.co/tWUuuXF864 https://t.co/duAOgZyFBg
>
> — Jake Williams (@MalwareJake) December 24, 2020