HOW OUR SPACE STATION WAS DESTROYED BY INSIDERS

It was not a good day. Neither for me nor the Empire. Not just because our space station exploded, but because we practically saw it coming. And we did nothing. Well, almost nothing. Blowing up planets and deploying perimeter defenses just doesn't cut it when the enemy is already inside.

I'm only alive today because I happened to be at the RSA conference on the day of the attack. I can already feel something tightening around my throat -- I don't expect today to turn into too many tomorrows…

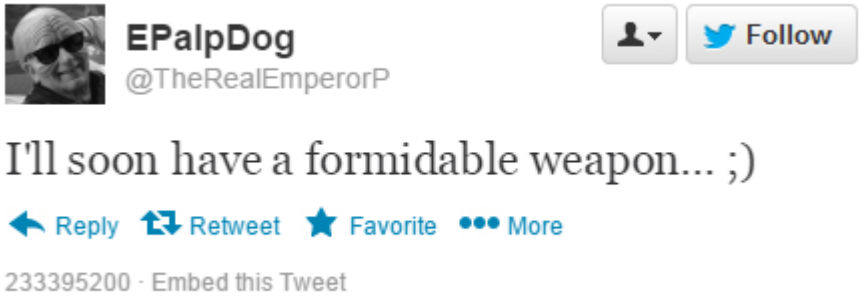
In what will be my last act as Space Station CISO, and most likely my last act as a sentient being, I will attempt to reconstruct the sequence of events that led to this disaster. Fortunately, our offsite backups

were secured at M-Iron Mountain, and I've been able to do some basic forensic analysis of the onboard systems and combine it with other historical records.

It begins…

Unfortunately, we all remember that our idea for the space station leaked much too early, making our job that much harder. I'm not making excuses here; just stating the facts.

Despite the efforts of our inter-planetary censorship net, our leader's tweet – meant to be a direct message to his mistress – had already gone viral. The secret was out.



The image he included with his tweet has been omitted so that we don't have to see it again.

It is my belief that this incident led to increased penetration efforts by our adversaries. Moving forward, I must reiterate my recommendation that all employees go through basic security training. Unfortunately, my investigation turned up additional failures to handle sensitive information correctly.

PART I

It has been said that almost every data disaster starts with an email. Ours may have started with a tweet, but leaked emails between our leader and Count D increased the damage exponentially.

Unfortunately, our leader's inbox was accessible to several of his assistants, and his admins frequently sent emails on his behalf. Worse, email was externally accessible via web, and two-factor authentication was not yet enabled.

Our investigation revealed that one of the assistant's accounts was compromised, and their account was used to read email exchanges that took place between our leader and the Count early in the design phase of the station. This sequence, for example, was read and then marked as unread using the assistant's account. The IP address of the computer accessing it was registered in a different star system – light years away from the assistant's actual workstation.

From: EP
Sent: Wednesday, November 25, 77 8:54 AM
To: CD
Subject: Project Happy Meal
Importance: High

What is the status?

P

Like me on facebook!

From: CD
Sent: Wednesday, November 25, 77 8:57 AM
To: EP
Subject: RE: Project Happy Meal
Importance: High

We're on schedule, my Lord. We've overcome the design issues with the tractor beam.

From: EP
Sent: Wednesday, November 25, 77 8:58 AM
To: CD
Subject: RE: Project Happy Meal
Importance: High

Excellent. Can you email me the latest schematics?

From: CD
Sent: Wednesday, November 25, 77 8:59 AM
To: EP
Subject: RE: Project Happy Meal
Importance: High

They're too big to email. Do you have a Dropbox account?

These early schematics are still stored in Dropbox, and worse, through careless use of public links were indexed, copied, and copies are now accessible via most search engines.

PART II

In addition to schematics, the attacker was able to mine our leader's emails to ascertain the names, nicknames and foibles of the generals who went on to oversee the construction of the station. One of these generals was the target of a spear-phishing attack that compromised his laptop.

From: EP@ds.mil.nb
To: gmt@ds.mil
Subject: Security Alert

Tark,

Check out this Roomba Cat video. It's hysterical.

P

The video website was compromised at the time, and when the general went to the site he was presented with a pop-up that said his computer had been infected. The pop-up prompted him to download and install the Windows Defender virus protection package, which he did.

Unfortunately, Windows Defender was itself malware. The malware quickly searched local disks and mapped drives with simple findstr commands for files that contained references to the Space Station:

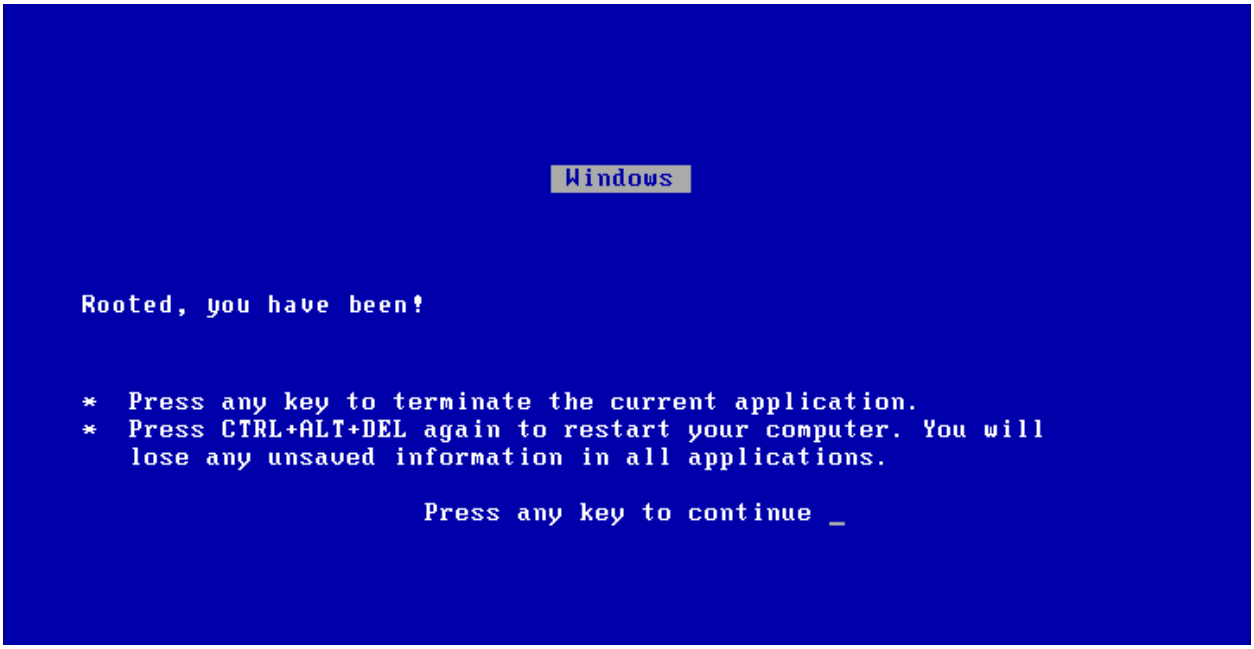
```
X:\> findstr /R ^[Dd]eath
```

Matching files included vendor quotes, contractual agreements, payment schedules and timelines. We believe these files were concatenated to several hex files and then exfiltrated over DNS.

PART III

The attackers used the General's workstation as a jumping off point to move laterally through our systems, and installed several very destructive programs that were executed on the morning of the attack.

The screenshot my team emailed me sent shivers down my spine:



PART IV - A NEW NOPE

Shortly after I learned of the attack, I mandated the use of biometric authentication mechanisms in all systems – fingerprints, iris scans and facial recognition. I was cautiously optimistic that this initiative would not only increase security, but also help me redeem myself as CISO – and possibly save my life. I bet our entire budget on it.

Then, a few minutes ago I received the following communication:

> ---
>
> **From: DV**
> **To: SSCISO**
> **Subject: Biometric authentication**
>
> Your expedient implementation was commendable. However, did you fail to consider that 90% of our employees are clones?
>
> ---

I have failed him for the last time…