Defending against Cyber Extortion

Transforming for Resilient Response

Gartner Symposium - 2023

Erik Gaston – CIO, VP Global Executive Engagement

TANIUM

Presenter

Erik Gaston

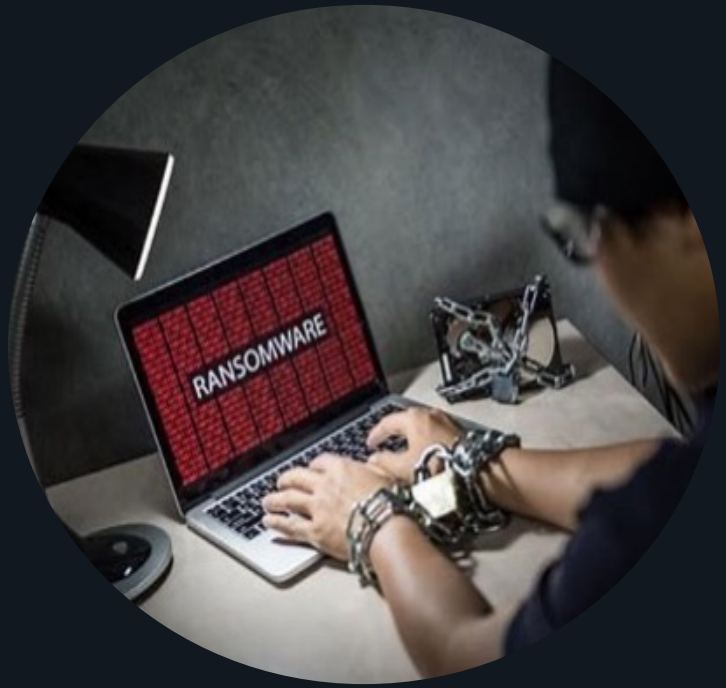
CIO, VP Executive Engagement

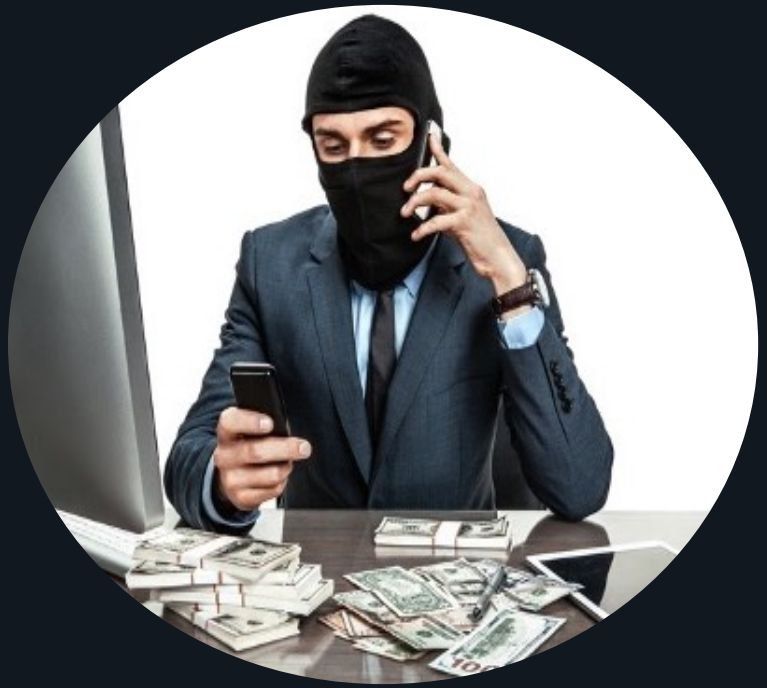
Tanium

Agenda

1. Current environment & the danger of conformity
2. How extortionists get initial access
3. The transformational starting point

From Ransomware to Extortion: Why Should We Care?





Only 1.9% of board directors representing S&P 500 companies have held relevant professional cybersecurity roles in the past 10 years

What are the Criminal Gangs Saying?

“I keep track of what researchers are saying … I follow some … because it’s always funny to see what they get wrong. [*****] is always good to get a laugh. The West always thinks that their technology is better than everyone else…”

“I want my developers to use post-quantum encryption to make it more secure.”

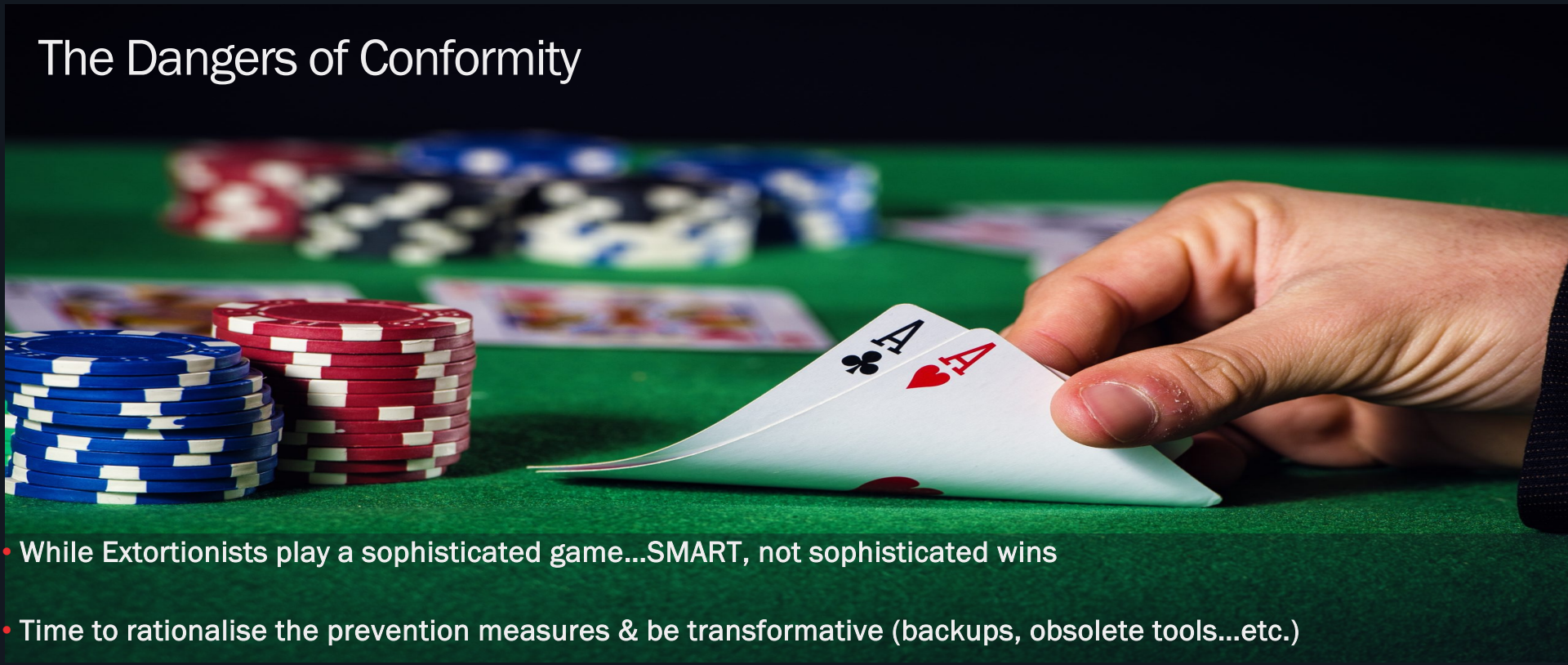
“… We know how to change our approach to always make money. That's why I decided that we need to move from a banking Trojan to providing extortion services. …the pandemic [messed] us up, and I realised that instead we need to move on to extortion. This is the only good way to make money now.”

“By the time they realise their money is gone, so are we.”

"Very soon I will be so rich that I will be able to buy my own island!”

Смелли of URSNIF – Banking trojan (RM2, Goziat, RM3, LDR4) author moved to generic backdoor (LDR4) in Oct 2022. Planning extortion 2023

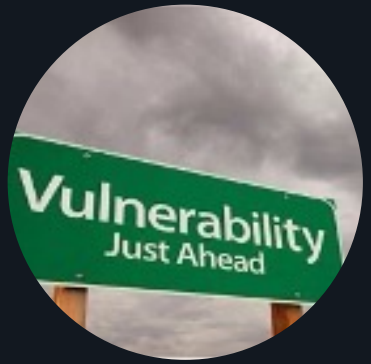
The Dangers of Conformity

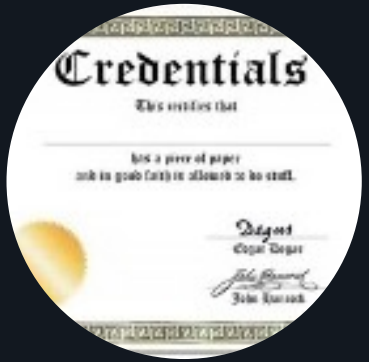


- While Extortionists play a sophisticated game…SMART, not sophisticated wins
- Time to rationalise the prevention measures & be transformative (backups, obsolete tools…etc.)
- Are you willing to call the bluff??? This is the danger of conformity at its best!
- No safety in doing what everyone else is doing…time to rethink the overall approach

How do Extortionists get Initial Access?

- Lightweight, disposable malware loaders emerged in 2022
- Infostealer malware contributed to the sale of over 2m credentials in one marketplace
- Exploitation of remote services replaced credential-based access as the most common access vector
- Nation-state activity has developed a more regional focus





What do we look like to...?

First...look at the situation from the outside-in & start with the problem

Attackers

End Users

Customers

Programmatic Hygiene is the Key to Prevention

- Establish key asset lifecycle programs

- Authentication and authorisation programs

- Lean on key foundational programs (IR /CR/PM/ DR / BCP)

- Automation and scalability programs

Managing Friction for Resiliency – How to Handle Extortion Threats

TANIUM

Key Takeaways

- The threat landscape is evolving, becoming more costly and devastating for organisations.
- "Transforming" not "conforming" is critical to be ready for these types of threats…Smart vs. Sophisticated!!
- Prevention is key and requires foundational programs to be implemented.

Thank you!

Erik Gaston
CIO, VP Executive Engagement

linkedin.com/in/erikgaston/

TANIUM