Illusions vs Reality

Jason Truppi – Director of EDR - @NotTruppi

JPMorgan Chase Hacki

By JESSICA SILVER-GREENBERG, MATTHEW

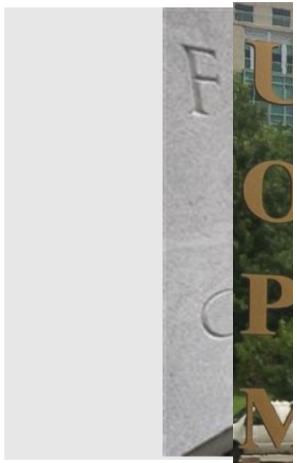
528

NY ju
of co

NEW YORK | E

Technology | Wed Jan 18, 2012 6

U.S. cha



People walk past the Fede
REUTERS/CHIP EAST

WANTED

Lizard Squad plans Christmas Day encore with Xbox, PlayStation attacks

Remember last year? The hacking group Lizard Squad, best known for online pranks and targeting gaming networks, took down PlayStation and Xbox on Christmas Day. Now, it's threatening to do the same this year, and the hackers have help.

By Fruzsina Eördögh, Correspondent | DECEMBER 24, 2015

Save for later

ntenced to Life

ers Infiltrated New

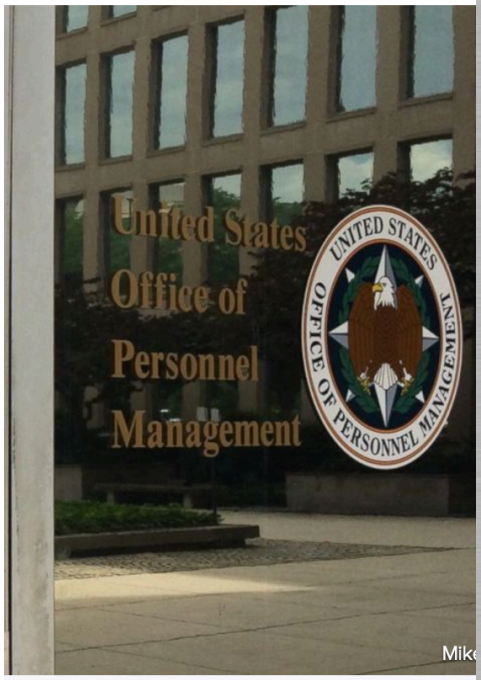
3

l system of small structure near

, Officials Say

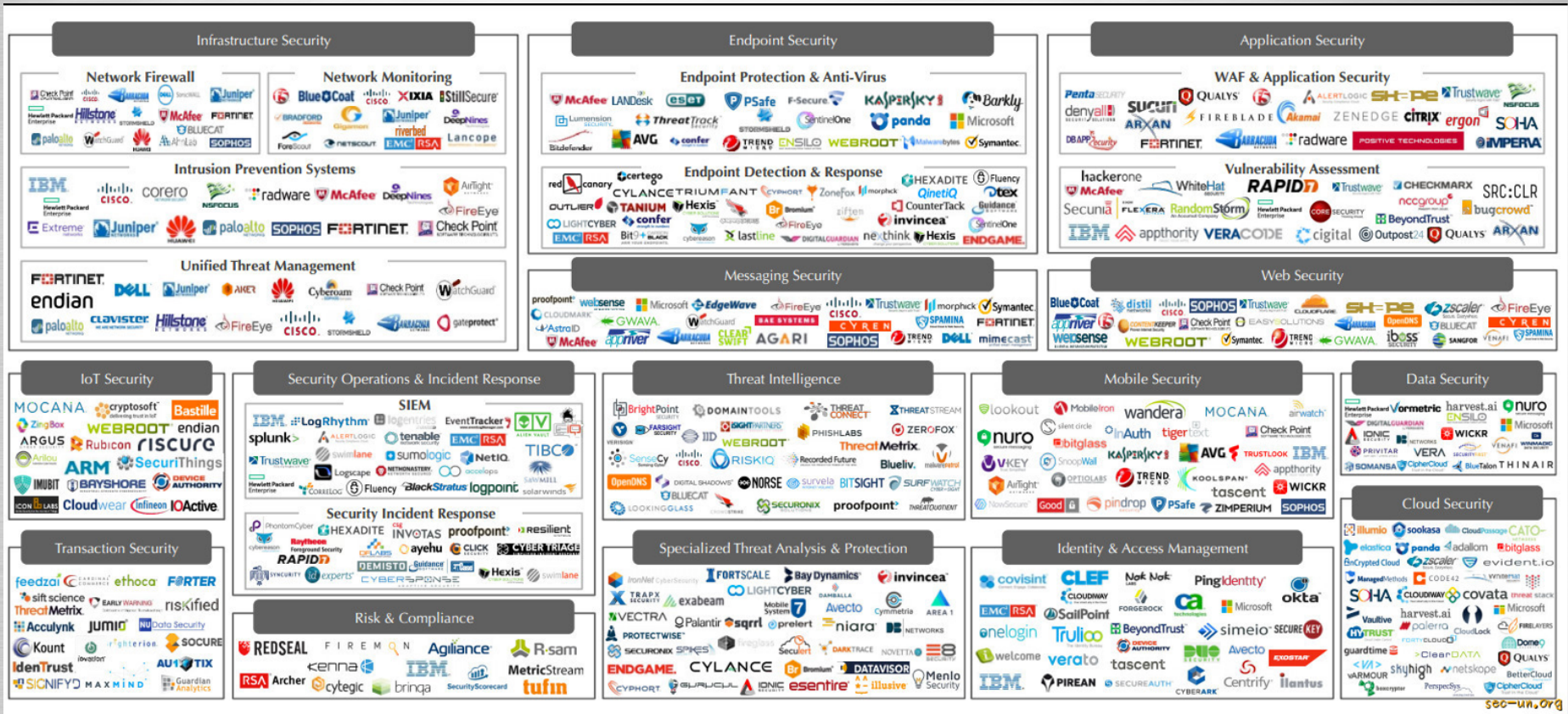
Share with Facebook

Share with Twitter



Parallels

- Visibility
- People Process Product
- Principles of Basic Hygiene
- Perimeter is Gone
- Need For Rapid Response
- Overwhelming Choices



Source: Momentum Partners.

sec-un.org

TANIUM™

TANIUM™

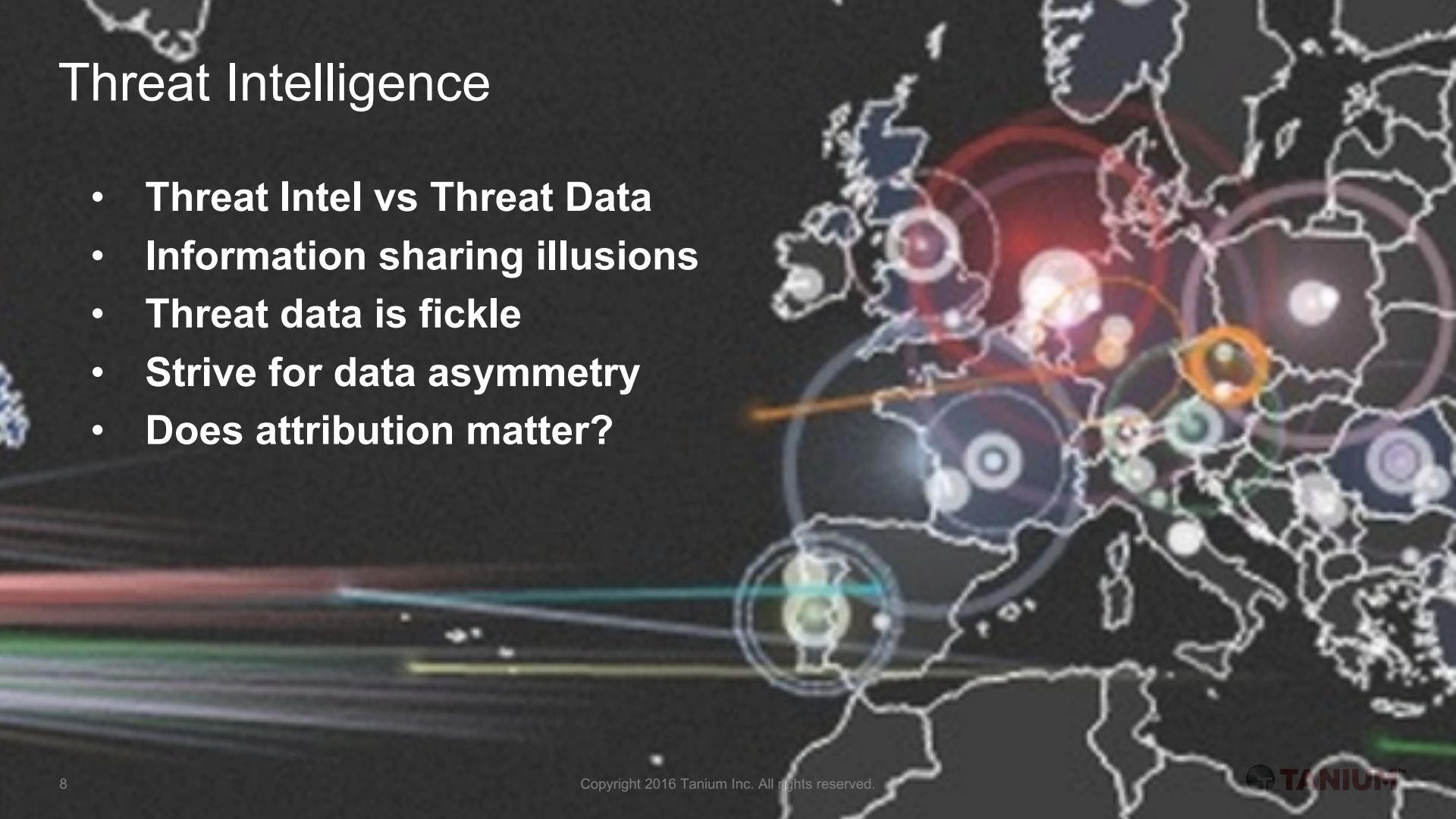
Rapid Response

- **Can we combat breach fatigue?**
- **No more security goldfish**
- **Tool consolidation**
- **IR teams are new or in development**
- **Processes are slow and cumbersome**
- **The need for valuable metrics?**
- **Automagical response**

Response Metrics

- **Solid playbooks**
- **Meantime to patch**
- **Time from alert to triage**
- **Time from triage to remediation and/or enforcement**
- **Minimize system recovery time**

Threat Intelligence



- **Threat Intel vs Threat Data**
- **Information sharing illusions**
- **Threat data is fickle**
- **Strive for data asymmetry**
- **Does attribution matter?**

Threat Actors

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain	Trusted insiders steal proprietary information for personal, financial, and ideological reasons	Nation-state actors conduct computer intrusions to steal state secrets and/or proprietary information from private companies	State and non-state terrorists create fear and impact life safety by attacking the computer systems that operate our critical infrastructure	Nation-state actors sabotage military and critical infrastructure systems to gain a tactical advantage in the event of a war

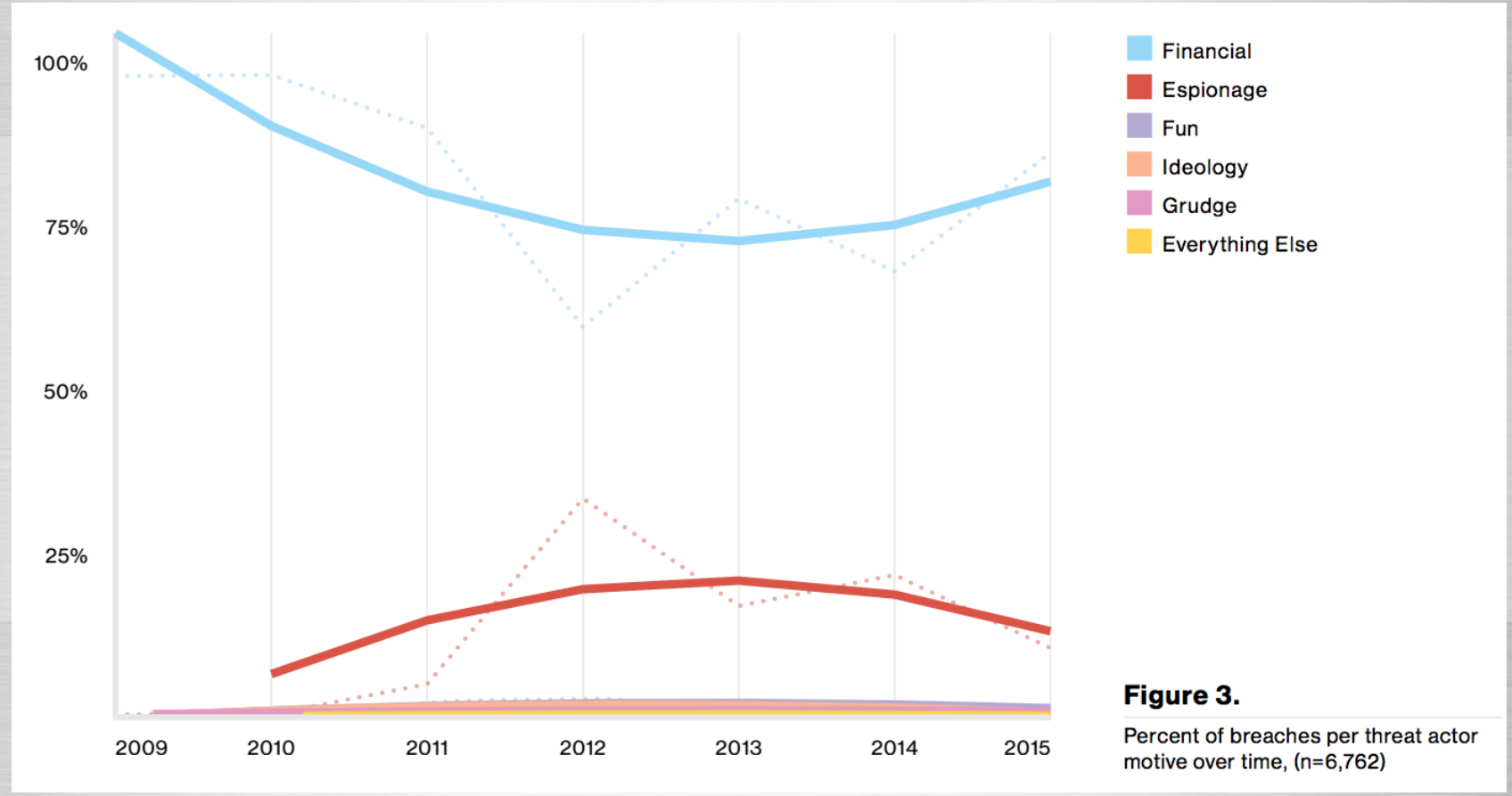


Figure 3.

Percent of breaches per threat actor motive over time, (n=6,762)

Compliance and Best Practices

- **Undue cost with minimal effect**
- **What's actually working?**
- **Who do you report to?**

PCI DSS COMPLIANT

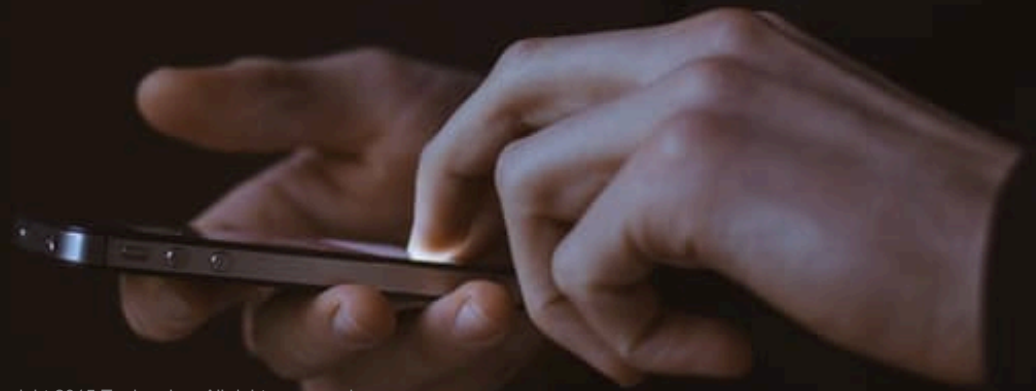
TANIUM™

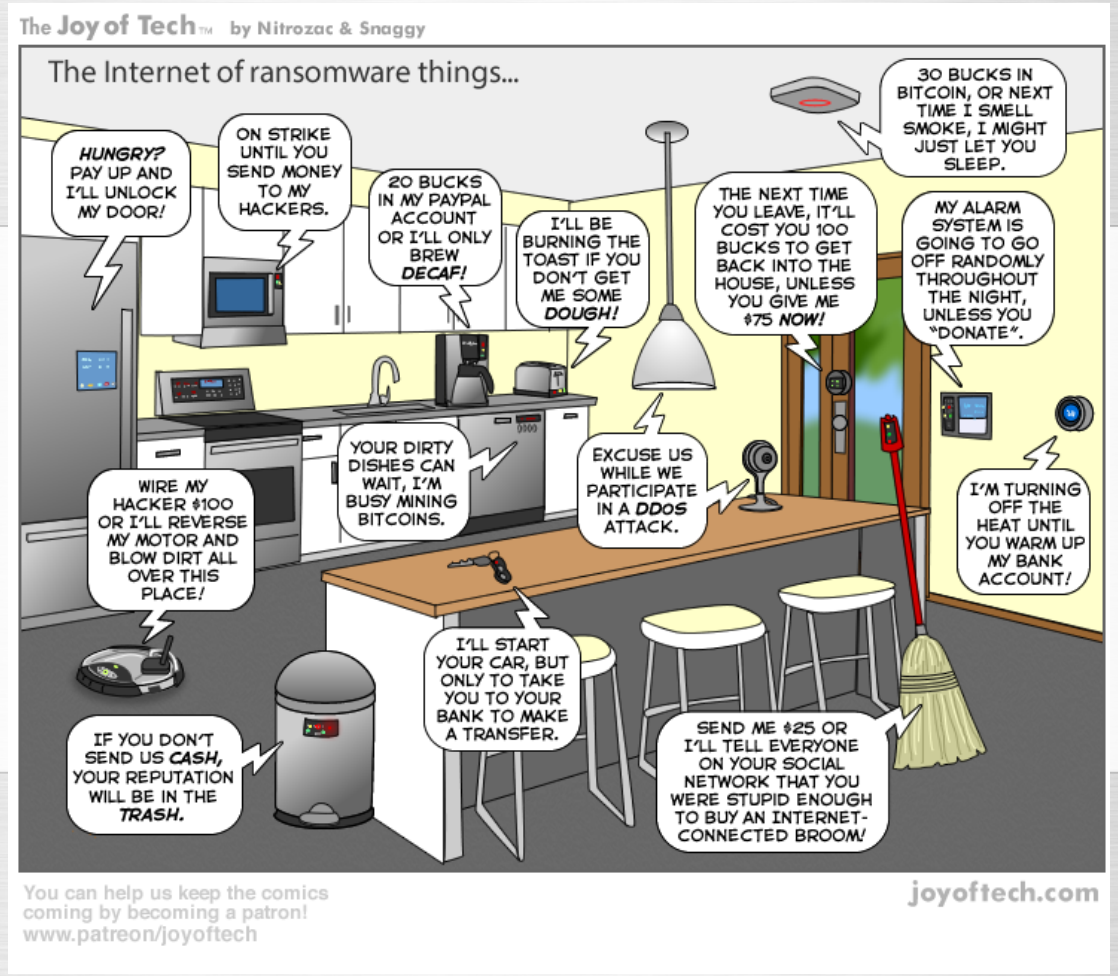
The Cloud

- Fear the cloud, the cost or the human?
- Is it secure?
- Who is liable?
- Is it reliable?
- Enhanced segmentation
- Identity management

Our Future

- **Application security**
- **Internet of Corruptible Things attacks**
- **Going dark**
- **Detection, investigation and remediation automation**
- **Biodata compromise**
- **Mobile vs desktop**




The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech
joyoftech.com

TANIUM™

Jason Truppi – Director of EDR
@NotTruppi