Threat Hunting Your Supply Chain

Jake Williams (@MalwareJake)
Rendition Infosec
www.rsec.us
@RenditionSec

$whoami

- Founder and President of Rendition Infosec
- SANS Senior Instructor and Course Author
- IANS Faculty
- Rally Security Co-Host
- Former NSA hacker, Master CNE operator, recipient of the DoD Exception Civilian Service Medal
- **Dislikes:** those who call themselves “thought leaders,” “crypto bros,” and anyone who **needlessly adds blockchain** to a software solution

Agenda

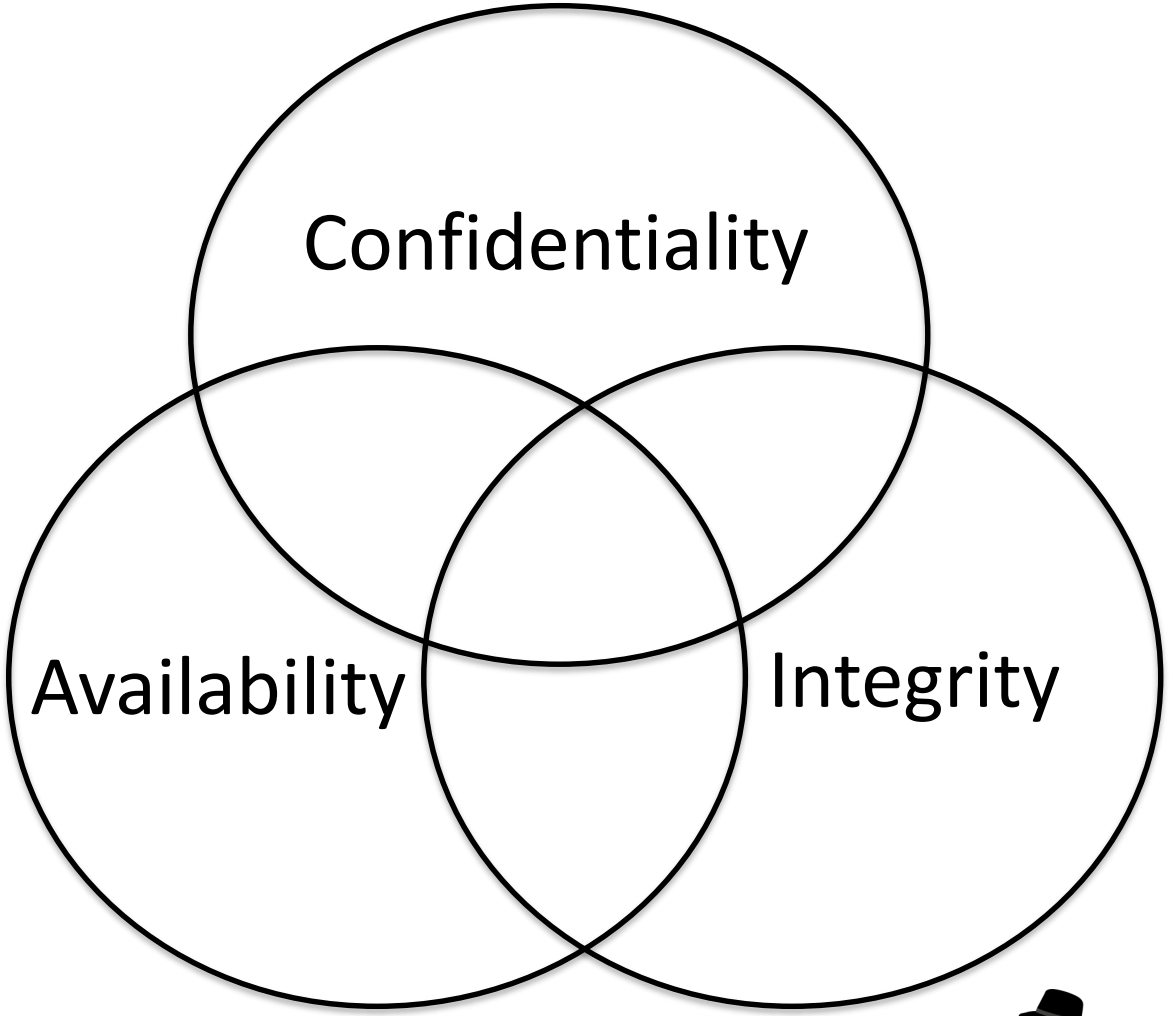
- Recent failures in supply chain risk assessment
  - Adobe
  - Snapchat
  - NotPetya
  - Others
- How to find threats even your vendors don’t know about

- Introducing SCREATH (Supply Chain Threat Hunting Framework)

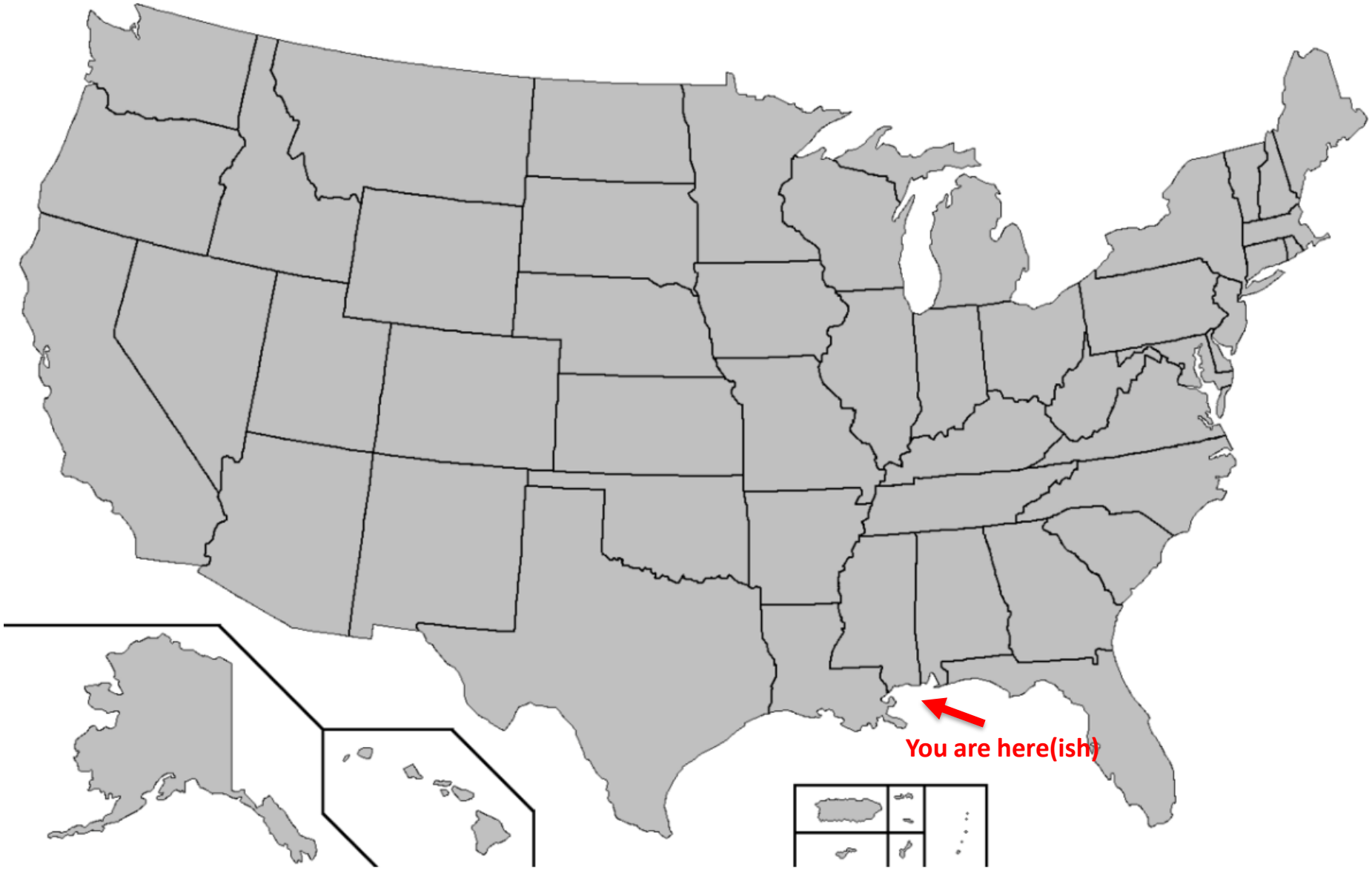
Supply Chain Security – it's all CIA

- Supply chain security is about:
  - Confidentiality
  - Integrity
  - Availability

- **NOT JUST CONFIDENTIALITY!**



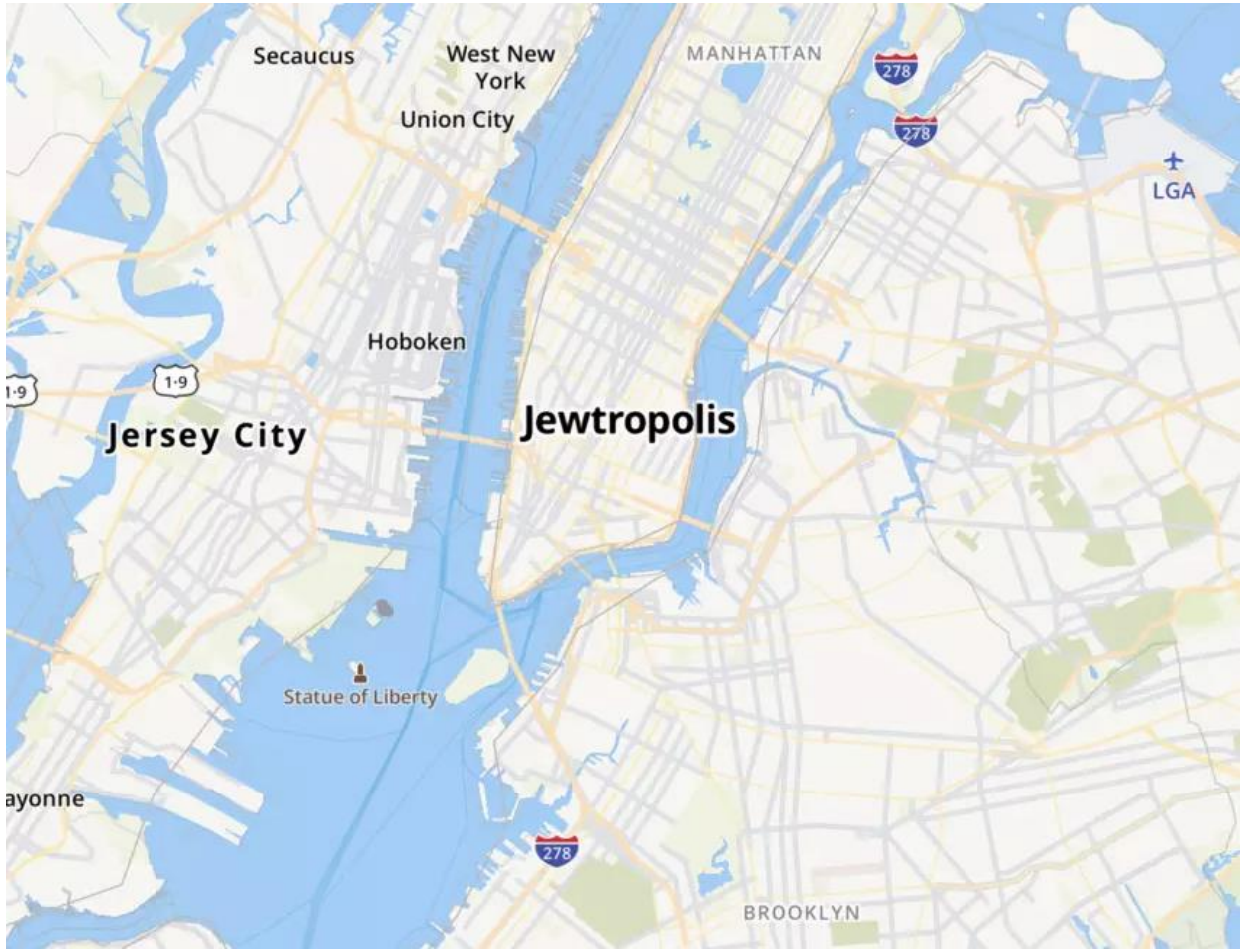
Who came the farthest to be here?



RENDITION INFOSEC
Cybersecurity by any legal means

Did anyone travel to the summit from NYC? (or this place)

- Snapchat and others were victims of a supply chain attack less than two weeks ago where Mapbox began mislabeling NYC



NotPetya

- Unless you were in a coma last year, you probably heard about the Russian attacks on Ukraine
  - The attack impacted much of Eastern Europe, Maersk, etc.

- Russian APT compromised the tax software MeDoc and used their software update mechanism to spread malware

- Malware was deployed through software update mechanisms
  - Third party software update mechanisms are notoriously difficult to secure and most vendors get this VERY wrong

NotPetya – MeDoc Server Room

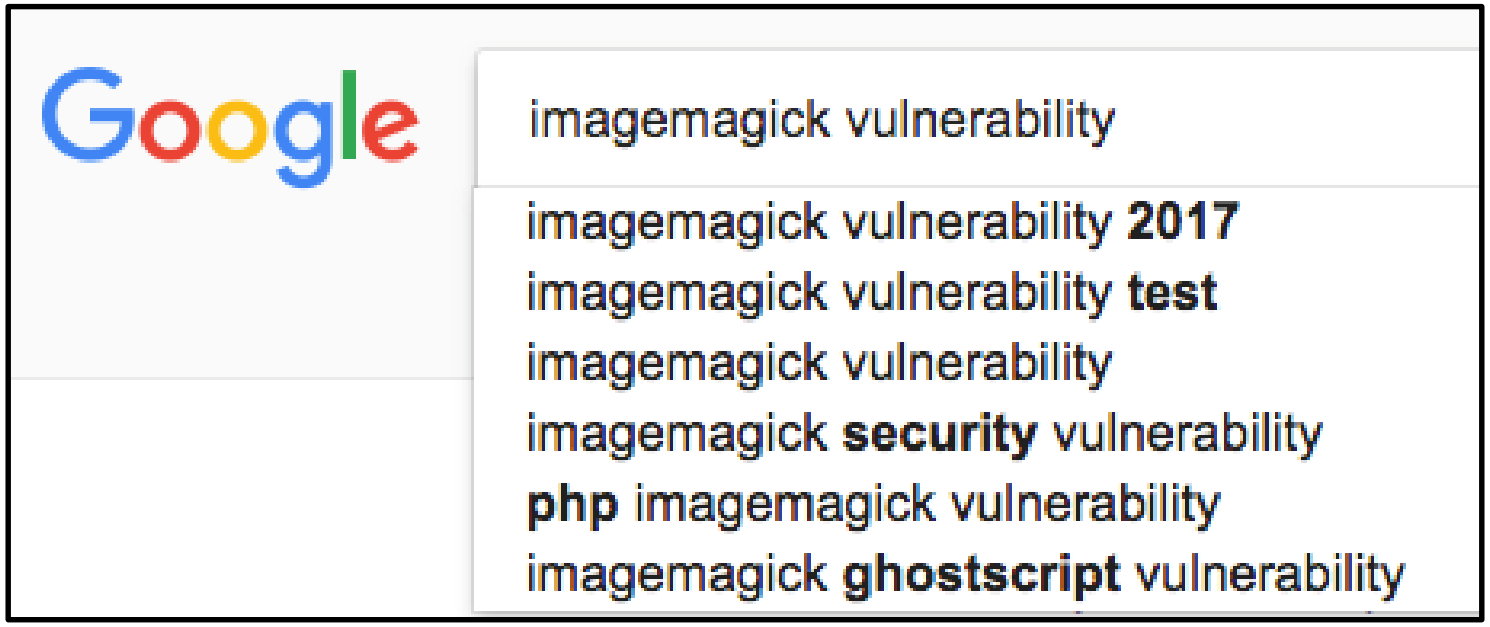
- It’s hard to imagine a company without adequate server room cooling (or fan covers) having invested in great security

- But when buying hardware, software, or services, we rarely get such an in-depth look at internal operations

- We need a supply chain risk evaluation framework

ImageMagick

- ImageMagick is an image processing library that is in all sorts of third party software
  - And is unfortunately very complex and very buggy
- Evaluating the security risk of ImageMagick could be as easy as using Google Autocomplete…



Do you have ImageMagick installed?

- This is probably harder to find an answer to than you think
  - Searching Google for “Projects using ImageMagick” doesn’t return anyone tracking a list of projects on the first few pages

- Performing vulnerability assessments, we’ve talked to lots of software vendors who deny using ImageMagick but really are
  - They’re probably not intentionally lying
  - They’re probably using a dependency that has a dependency on ImageMagick too
  - Unraveling the software supply chain isn’t easy…

Adobe Acrobat Vulnerabilities

- Dig into Adobe's Acrobat Reader and you'll find all sorts of open source libraries that are included
  - Open source is not inherently less secure, but is easier to track usage

Module	Description	Open Source Project
Axsle.dll	XSLT Backend	Sablotron
AcroForm.api	XFA (Forms)	libpng, libtiff
Escript.api	JavaScript (grumble)	Spidermonkey
ImageConversion.api	PDF Conversion Engine	libpng, libtiff, libjpeg

Other Supply Chain Fails

- MEGA's Hijacked Browser Plugin

> signatures where possible. Unfortunately, Google decided to disallow publisher signatures on Chrome extensions and is now relying solely on signing them automatically after upload to the Chrome webstore, which removes an important barrier to external compromise. MEGAsync and our Firefox extension are signed and hosted by us and could therefore not have fallen victim to this attack vector. While

- CCleaner
- NPM left-pad
- C[illegible]t

Supply Chain Threat Hunting

Finding threats even the vendor doesn’t know about…

Threat Hunting

- Threat hunting starts not by assuming compromise, but assuming **the possibility of** compromise
- Doing threat hunting right requires lots of data to find anomalies
  - Remember: if there was a signature, it would have already been detected. Most good threat hunting is done by detecting anomalies
- My top threat hunting data sources:
  - DNS request/response logs
  - Netflow
  - Proxy logs

Supply Chain Threat Hunting

- We should be threat hunting vendors the same way we threat hunt in our own networks
  - The problem is, what data can we use?
- Ask a vendor if they're threat hunting – they know the answer.
- Go to your average vendor and ask for some data to do threat hunting yourself:
  - DNS request/response logs
  - Netflow
  - Proxy logs
  - Literally any other source data you ask for

How can we threat hunt our supply chain?

- Obviously, the data we really want isn't available
  - In every other part of life, we use the data we can see to infer what we can't see
- If you need someone to hold your wallet for a few minutes, who are you most likely to choose?

Where there's smoke…

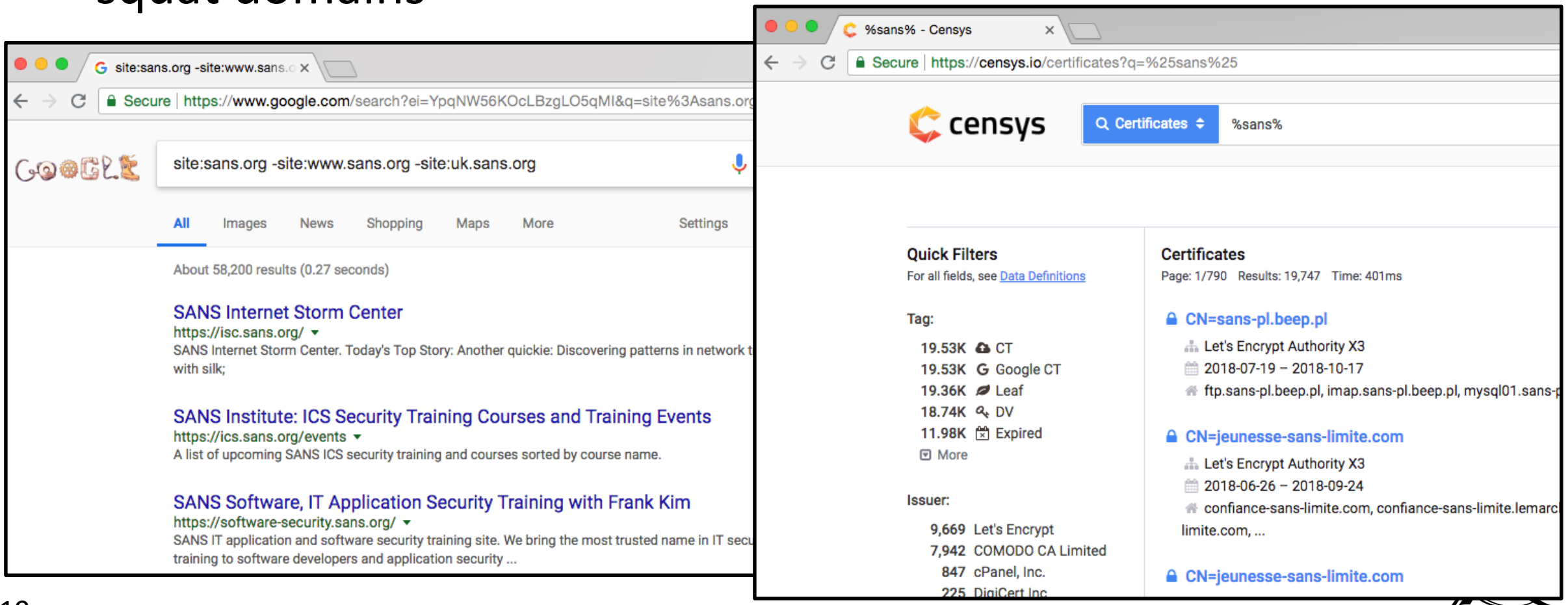
- To some extent, supply chain threat hunting is an extension of Broken Window Policing policies
  - "Where there's smoke, there's usually fire"
- Assuming that smoke -> fire is generally a bad idea
- When the fire is being intentionally hidden, all you can go by is the smoke…

What does “supply chain smoke” even look like?

- Vendors have a financial incentive to obscure “supply chain smoke” as much as possible
  - Most vendors will most provide baseline information (e.g. has the product undergone a 3rd party pentest) when asked
  - But they seldom volunteer this same information
- OSINT is required to see what they don’t want you to see…
  - Publicly available data
  - Document Metadata
  - Self-assessment questionnaires
  - Social Media

Monitor Domains

- Set up regular Google searches to find new subdomains and typo squat domains



Monitor Leaked Emails

- If your Cyber Threat Intelligence team is already downloading dumps, look for the emails of your vendors in the same dumps
  - **Get signoff** from your legal counsel before downloading dumps
- Consider the source of the dump in evaluating reliability
- If the dump isn't work related, that probably implies loose enforcement of acceptable use policies
  - Anecdotally, we know that failure to comply with acceptable use policies is a proximate cause for many breaches
  - This does **not** establish a solid causal relationship

Monitor DNS

- It is very rare for the DNS server IP address for a domain to change
  - If the DNS server for a domain changes, it may be the result of an attack on the domain owner

- Some vendors use their domain registrar's DNS servers
  - Attackers who compromise the registrar DNS control panel can add new subdomains without changing the DNS server IP
  - Passive DNS can show those domains once they are used operationally by the attacker

Monitor BGP

- This requires a bit more information about the target organization
  - BGP hijacks for offensive operations used to be largely theoretical
  - Lately, either we're looking for it more or it's happening more
- Most organizations aren't monitoring their own IP ranges for BGP hijacking attacks
- Doing this right requires knowing the vendor's IP ranges as well as the IP ranges of their suppliers/customers
  - Probably not feasible on a large scale

Monitor CTI Feeds

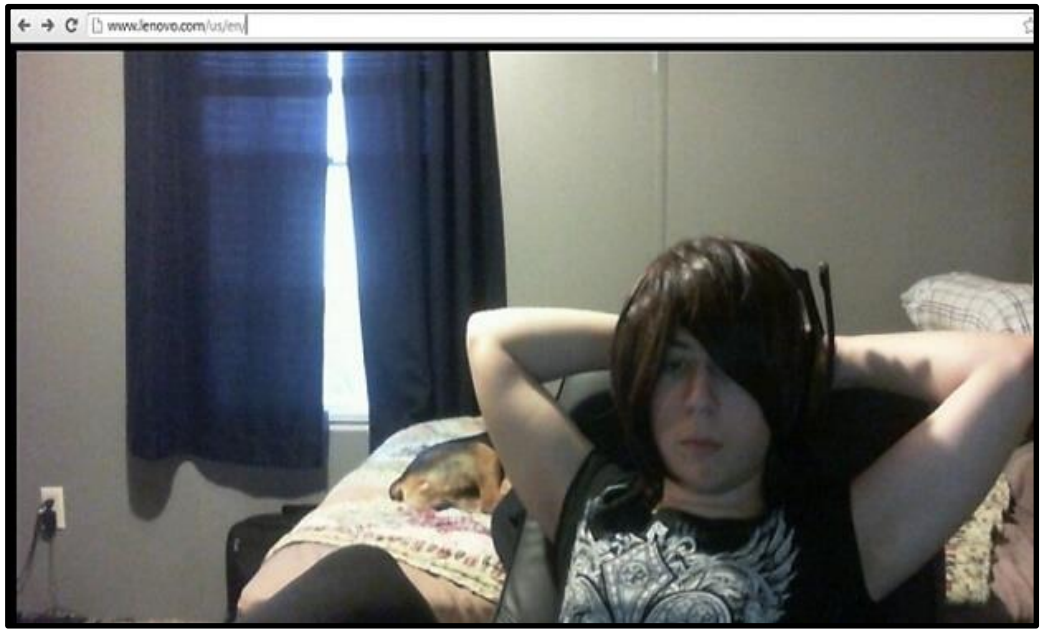
- This seems incredibly basic, but many vendors don't monitor CTI feeds for their own domains and IP ranges
  - Set these up to be monitored just the same as your own

- **Caution:** we've seen cases where DoS attacks are attempted by adding non-malicious domains/IPs to threat feeds
  - Just like anything else, investigate and respond appropriately
  - Know the reputation of the threat feeds you're using

Defaced Websites

- Monitoring the vendor's website for evidence of defacement is an excellent early warning sign of lax security posture
  - Luckily, this is easy to do and probably doesn't require any signoff from in-house legal counsel
- The website fluxguard.com lets you monitor up to 75 pages for free

Lenovo website, 2015



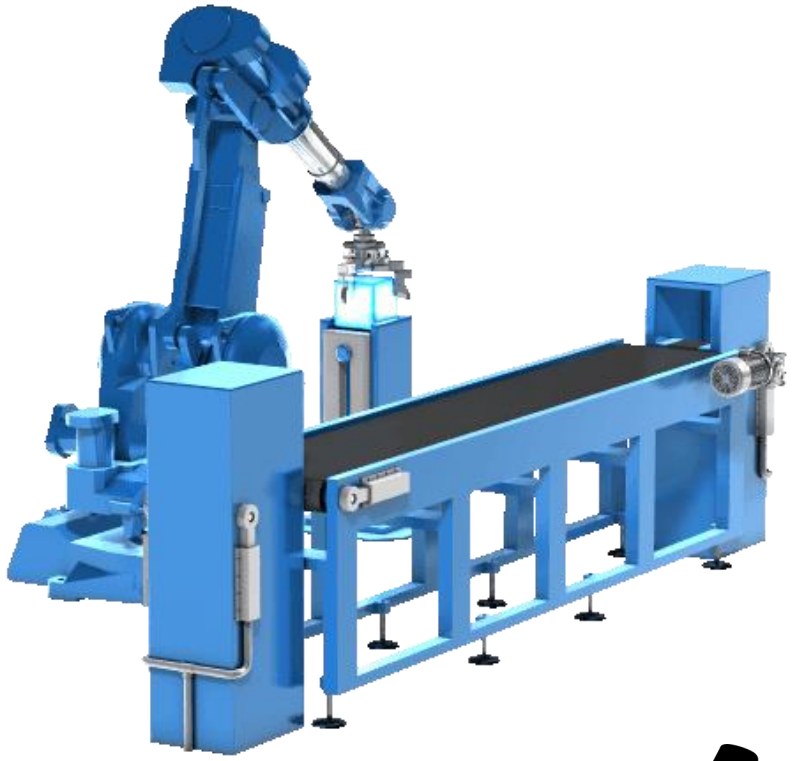
Evaluating Supply Chain Risks

Evaluating supply chain risks

- By performing good risk analysis, you may be able to avoid a number of supply chain threats in the first place
- MITRE recently completed a Supply Chain Security Strategy report
  - http://bit.ly/deliver-uncompromised
  - Unfortunately, this is written at national policy level and not really applicable for our needs
- The industry needs a standardized way to evaluate the supply chain risk posed by a vendor
  - Right now, it is very difficult to perform an apples-to-apples comparison

Introducing SCREATH

- SCREATH is an attempt to introduce a framework for standardizing supply chain risk evaluation
  - **S**upply
  - **C**hain
  - **R**isk
  - **E**valuation,
  - **A**nalysis, and
  - **T**hreat
  - **H**unting



SCREATH Principles

- Every component, no matter how well secured, must add risk
- No amount of effort can completely eliminate that risk
- Activities have both positive and negative weights, but no product can have a negative SCREATH score

- SCREATH is in version 0.1
  - We still need feedback for the score weighting in SCREATH
  - www.renditioninfosec.com/screath

Thanks for attending!

That’s all folks

@MalwareJake

@RenditionSec

www.rsec.us