NDC { London }

Securing the Software Supply-Chain

Niels Tanis

Who am I?

- Niels Tanis
  - Security Researcher @ Veracode
  - Background in .NET Development
  - Application Security Consultancy
  - Pen-testing & Ethical Hacking
  - ISC² CSSLP

The Rise of Software Supply-Chain Attacks

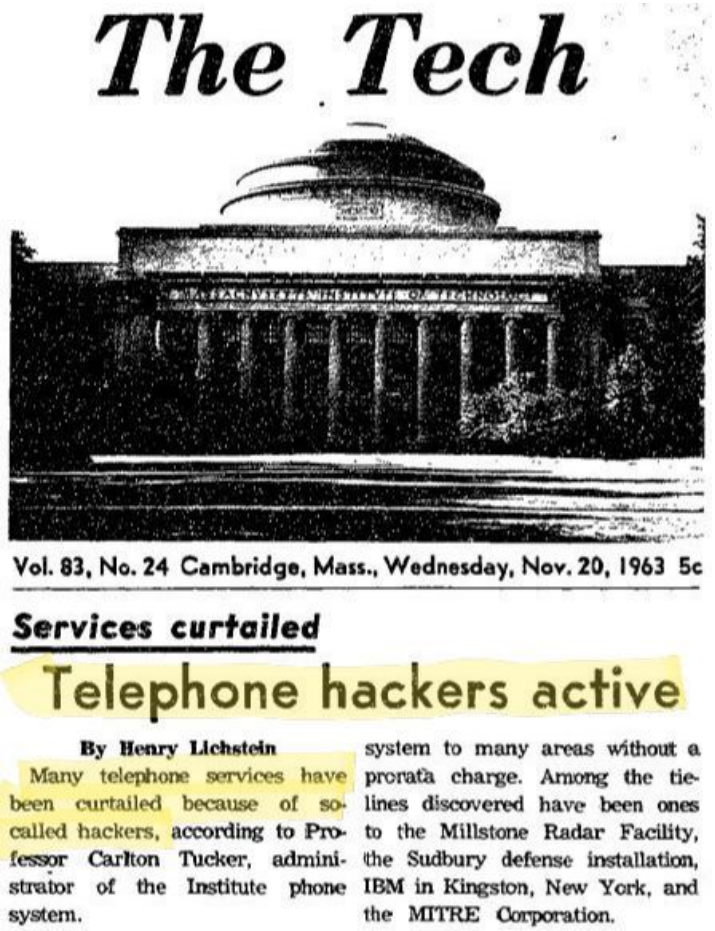
How Secure is your .NET Application?

Agenda

- Hacker History
- Definition Software Supply-Chain
    - Development of .NET application
    - Building / Releasing / Deploying
- Securing our Software Supply-Chain
- Conclusion and Q&A

Hacking History

- Started out with phreaking in late ‘50-’60



The Tech

Vol. 83, No. 24 Cambridge, Mass., Wednesday, Nov. 20, 1963 5c

Services curtailed

Telephone hackers active

By Henry Lichstein

Many telephone services have been curtailed because of so-called hackers, according to Professor Carlton Tucker, administrator of the Institute phone system.

system to many areas without a prorata charge. Among the tie-lines discovered have been ones to the Millstone Radar Facility, the Sudbury defense installation, IBM in Kingston, New York, and the MITRE Corporation.

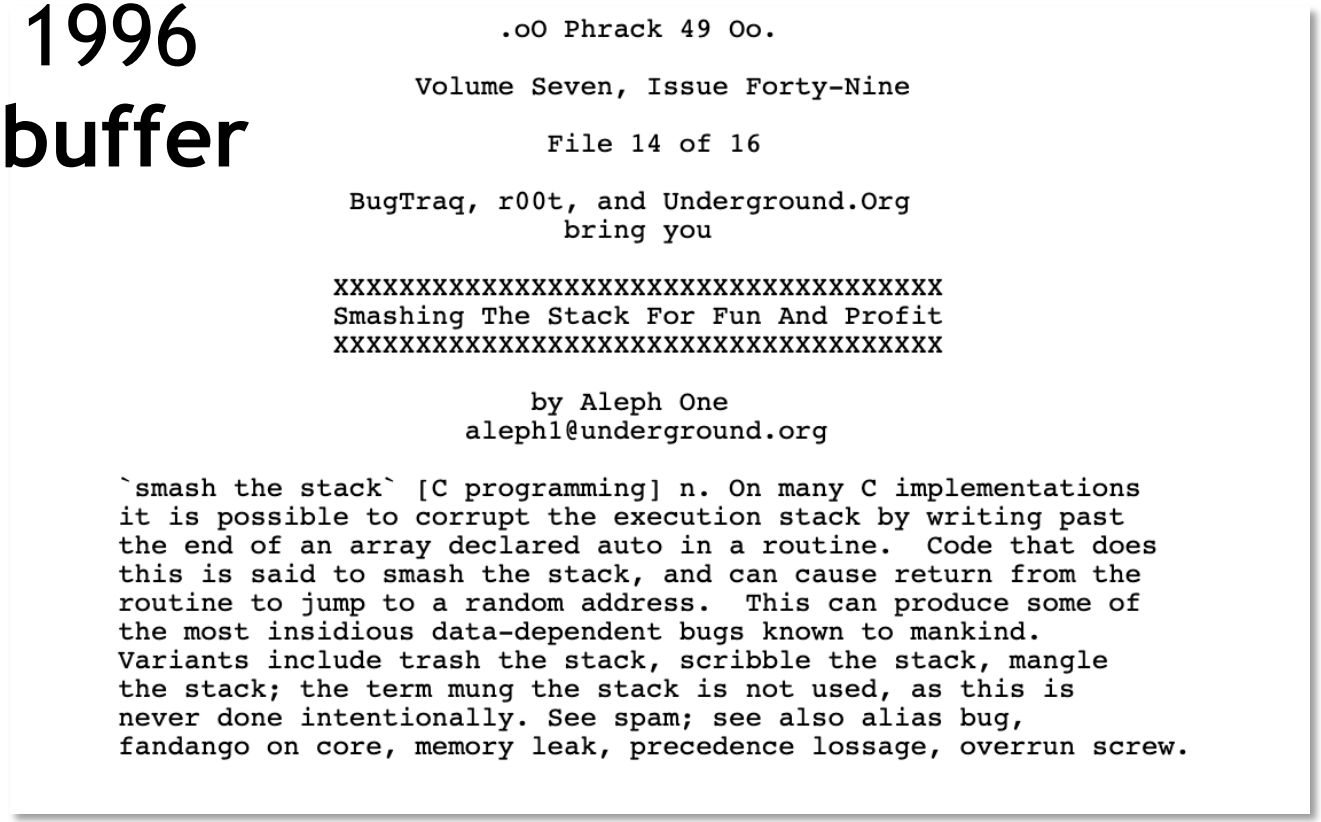
Getting connected!

- SATAN (**S**ecurity **A**dministrator **T**ool for **A**nalyzing **N**etworks) by Wietse Venema and Dan Farmer in 1995.
- NMAP (Network Mapper) by Gordon Lyon in 1997

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-14 11:05 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
25/tcp   filtered smtp
80/tcp   open     http
9929/tcp open     nping-echo
```

Smashing the Stack…

- Phrack #49 in November 1996 **Aleph One** wrote about **buffer overflows**



.oO Phrack 49 Oo.

Volume Seven, Issue Forty-Nine

File 14 of 16

BugTraq, r00t, and Underground.Org
bring you

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Smashing The Stack For Fun And Profit
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

by Aleph One
aleph1@underground.org

`smash the stack` [C programming] n. On many C implementations it is possible to corrupt the execution stack by writing past the end of an array declared auto in a routine. Code that does this is said to smash the stack, and can cause return from the routine to jump to a random address. This can produce some of the most insidious data-dependent bugs known to mankind. Variants include trash the stack, scribble the stack, mangle the stack; the term mung the stack is not used, as this is never done intentionally. See spam; see also alias bug, fandango on core, memory leak, precedence lossage, overrun screw.

SQL Injection

- Phrack #54 in December 1998
  Rain Forest Puppy wrote
  about **SQL injection**

```
----[  ODBC and MS SQL server 6.5

Ok, topic change again.  Since we've hit on web service and database stuff,
let's roll with it.  Onto ODBC and MS SQL server 6.5.

I worked with a fellow WT'er on this problem.  He did the good thing and told
Microsoft, and their answer was, well, hilarious.  According to them,
what you're about to read is not a problem, so don't worry about doing
anything to stop it.

- WHAT'S THE PROBLEM?  MS SQL server allows batch commands.

- WHAT'S THAT MEAN?  I can do something like:

        SELECT * FROM table WHERE x=1 SELECT * FROM table WHERE y=5

Exactly like that, and it'll work.  It will return two record sets, with each
set containing the results of the individual SELECT.

- WHAT'S THAT REALLY MEAN?  People can possibly piggyback SQL commands into
your statements.  Let's say you have:

        SELECT * FROM table WHERE x=%%criteria from webpage user%%
```

Code Red & SQL Slammer

- Microsoft Internet Information Server, July 2001

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

Bill Gates - Email to all MS FTE

BILL GATES BUSINESS 01.17.02 12:00 PM

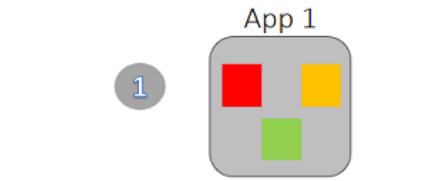
Bill Gates: Trustworthy Computing

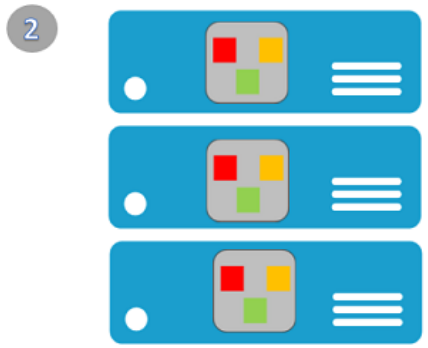
*This is the e-mail Bill Gates sent to every full-time employee at Microsoft, in which he describes the company's new strategy emphasizing security in its products.*From: Bill Gates
Sent: Tuesday, January 15, 2002 5:22 PM
To: Microsoft and Subsidiaries: All FTE
Subject: Trustworthy computing

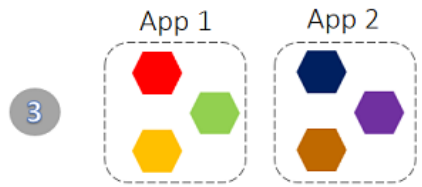
Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that

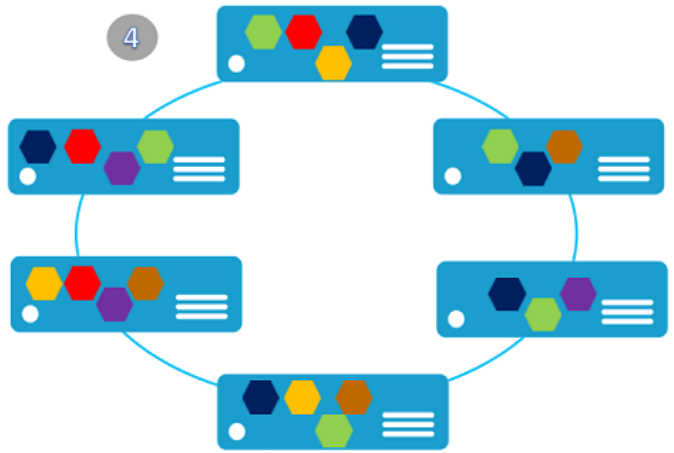
Changes in Software Architecture

- Monolith
- Microservices
- Serverless

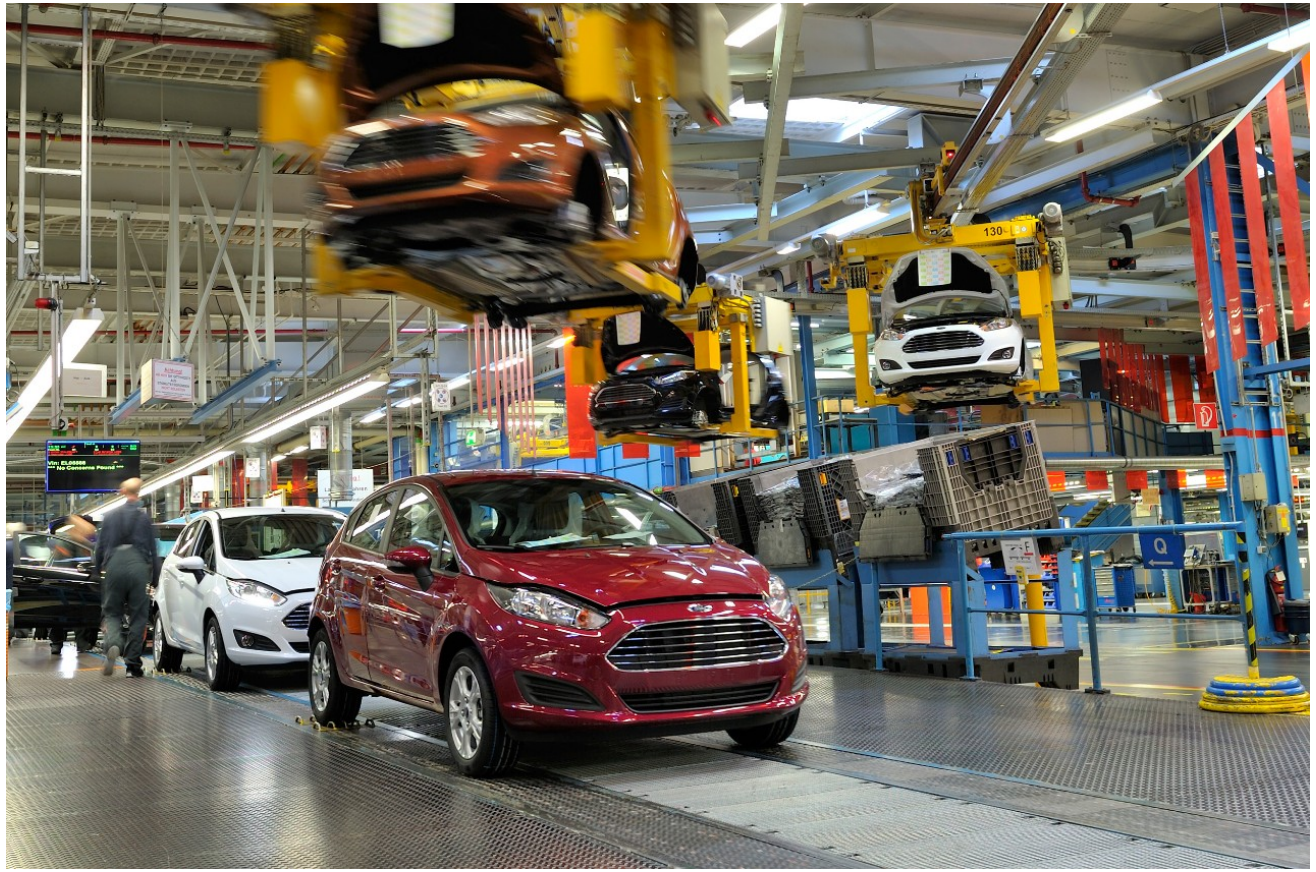




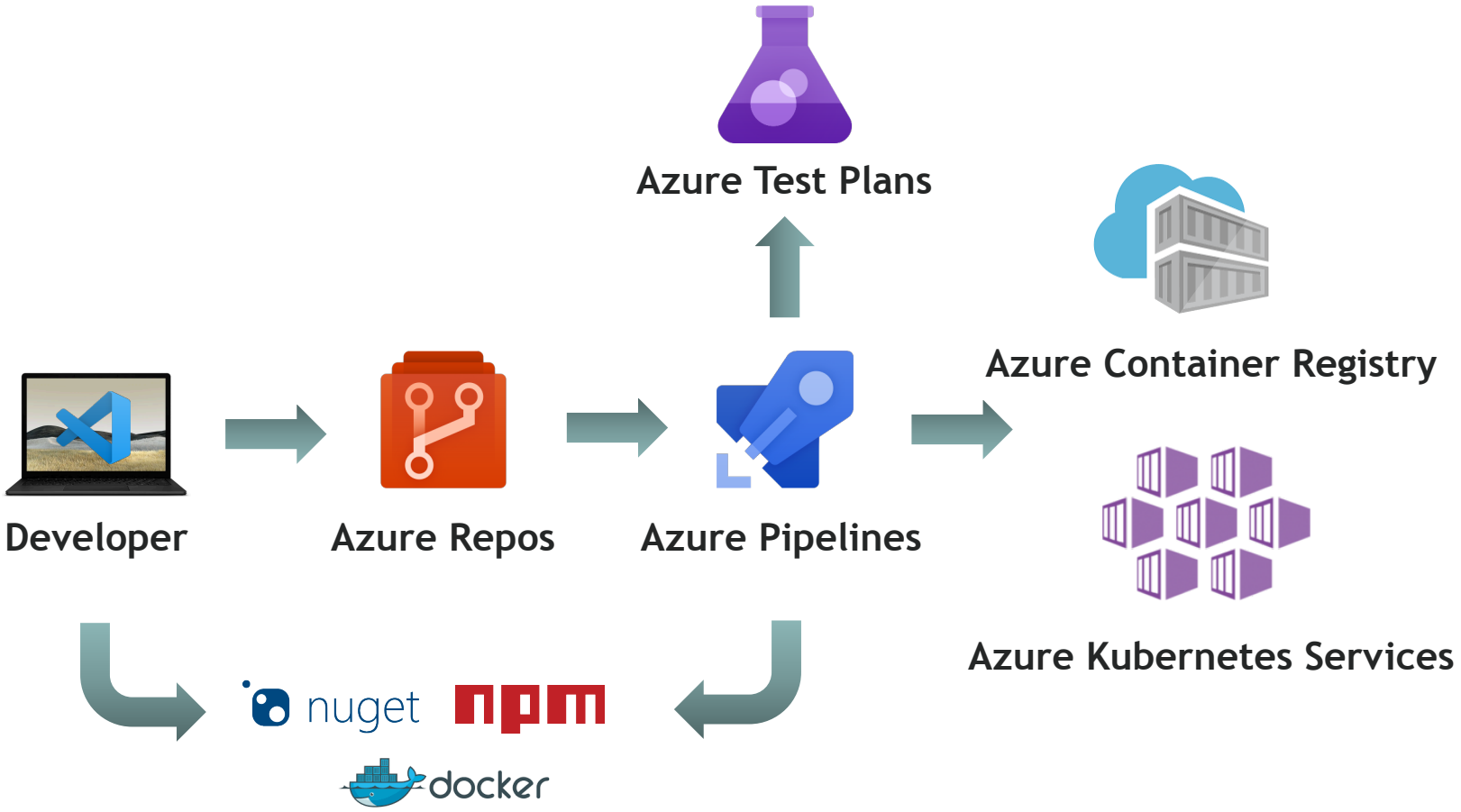




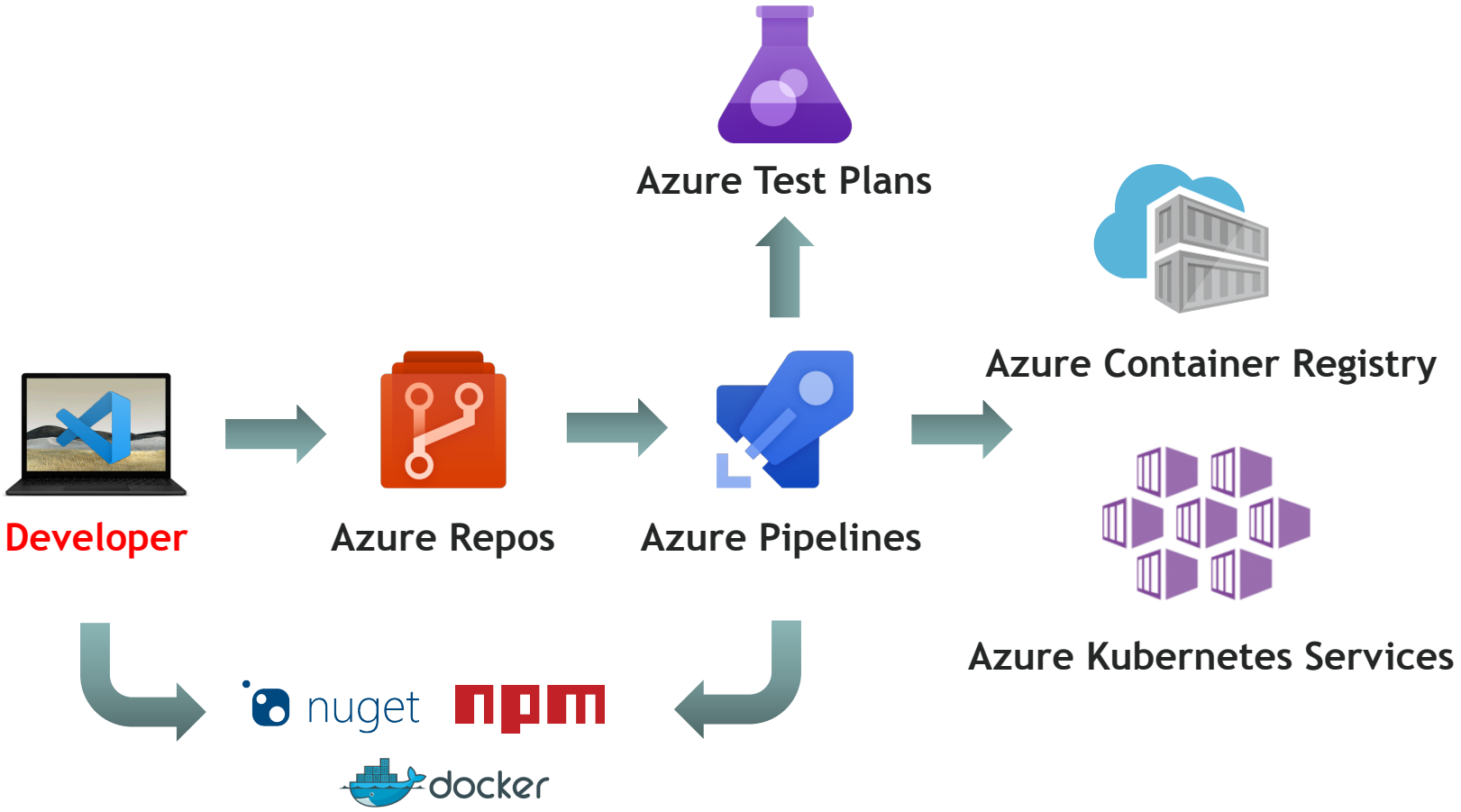
What is a Supply Chain?



Software Supply Chain

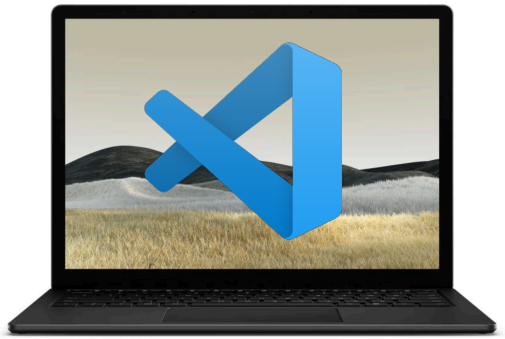


Software Supply Chain

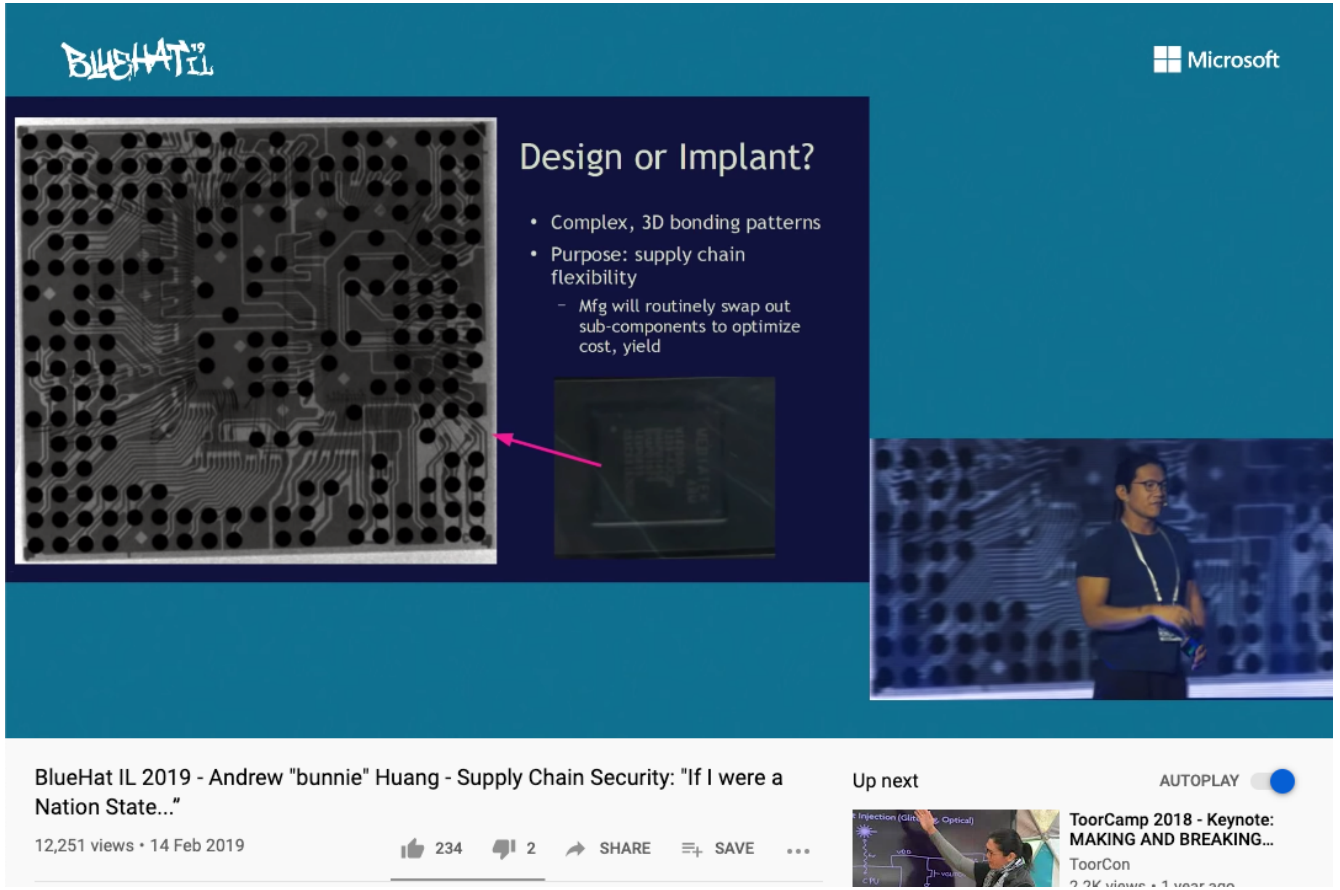


Development Machine

- Secure Boot & Trusted Platform Module (TPM)
- Encrypt disk, harden operating system install updates
- But can you trust the hardware?



Hacking Hardware



Development Machine

- Installs on machine – HomeBrew on Mac

README.md

Homebrew (un)installer

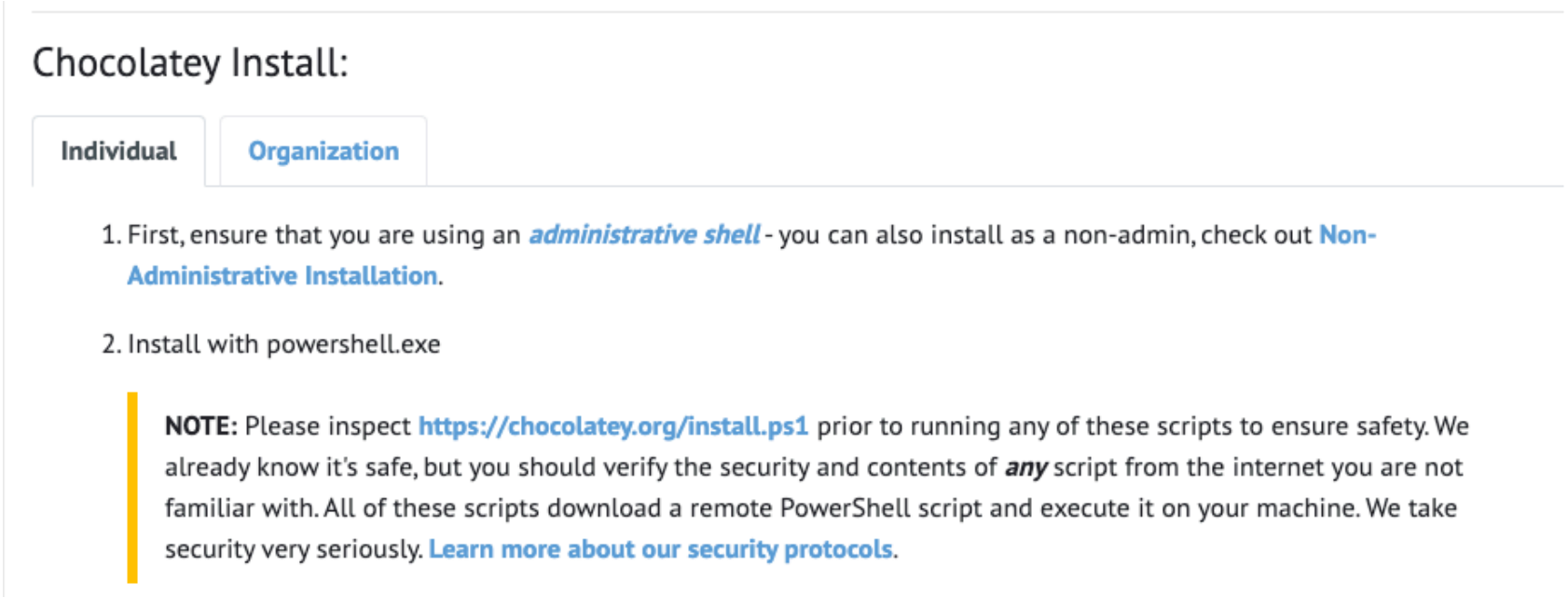
Install Homebrew

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install.sh)"
```

More installation information and options at https://docs.brew.sh/Installation.html.

Development Machine

- Installs on machine – Chocolately on Windows



Chocolatey Install:

Individual | Organization

1. First, ensure that you are using an *administrative shell* - you can also install as a non-admin, check out Non-Administrative Installation.

2. Install with powershell.exe

> **NOTE:** Please inspect https://chocolatey.org/install.ps1 prior to running any of these scripts to ensure safety. We already know it's safe, but you should verify the security and contents of ***any*** script from the internet you are not familiar with. All of these scripts download a remote PowerShell script and execute it on your machine. We take security very seriously. Learn more about our security protocols.

Octopus Scanner - NetBeans

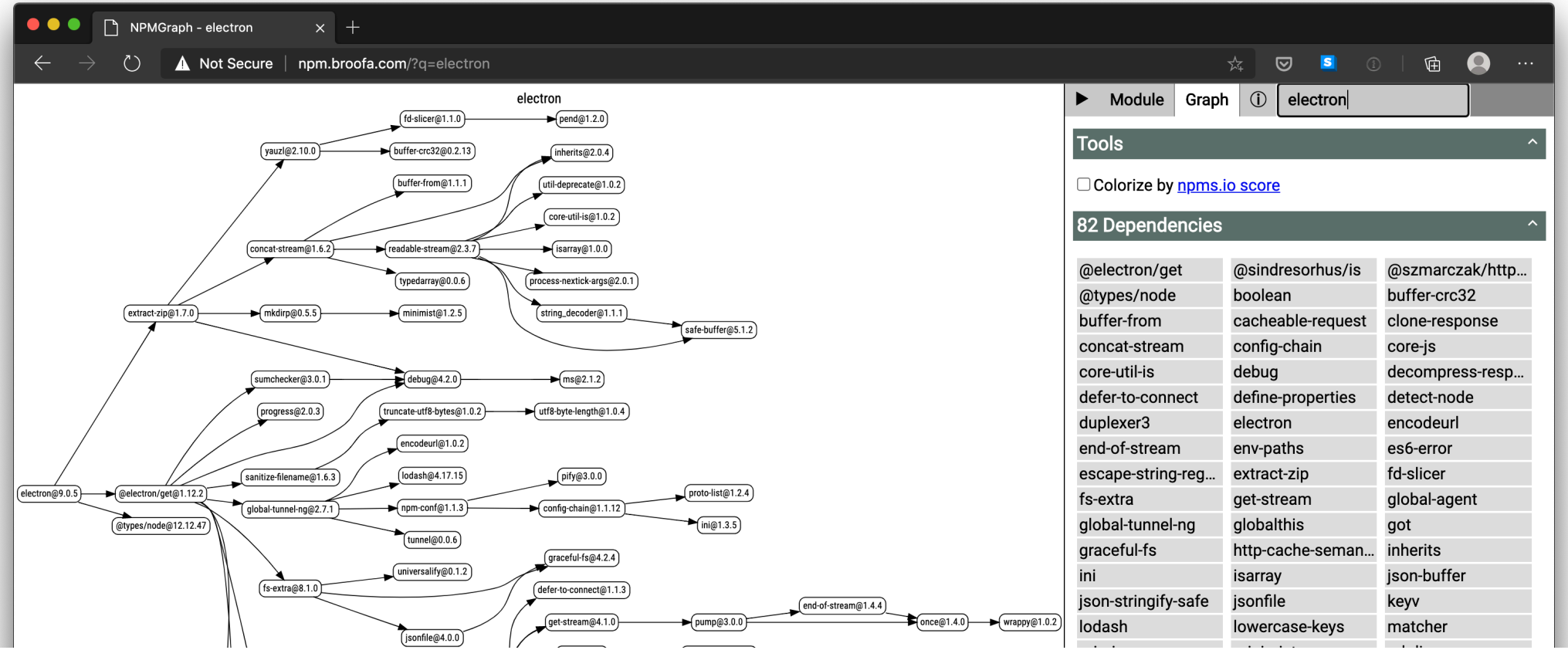
May 28, 2020

The Octopus Scanner Malware: Attacking the open source supply chain

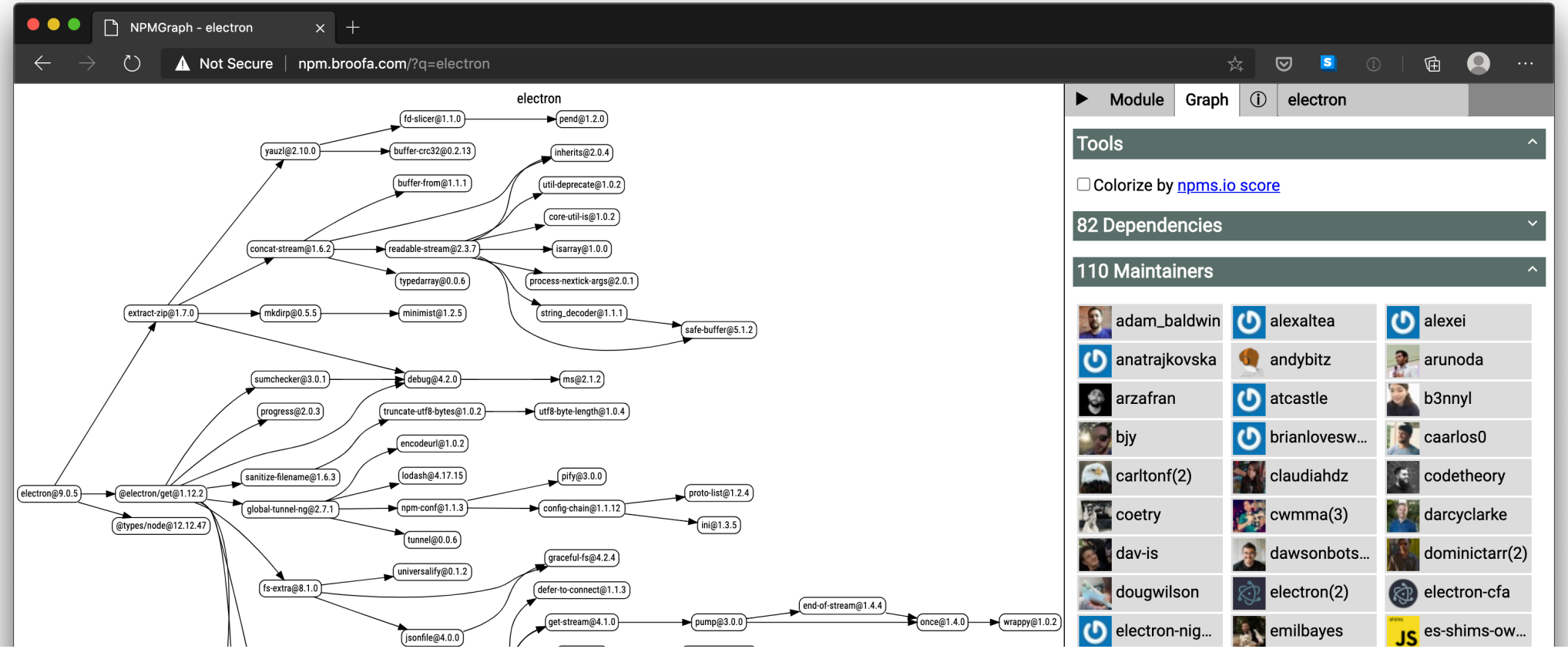
Alvaro Muñoz

Securing the open source supply chain is an enormous task. It goes far beyond a security assessment or just patching for the latest CVEs. Supply chain security is about the integrity of the entire software development and delivery ecosystem. From the code commits themselves, to how they flow through the CI/CD pipeline, to the actual delivery of releases, there's the potential for loss of integrity and security concerns, throughout the entire lifecycle.

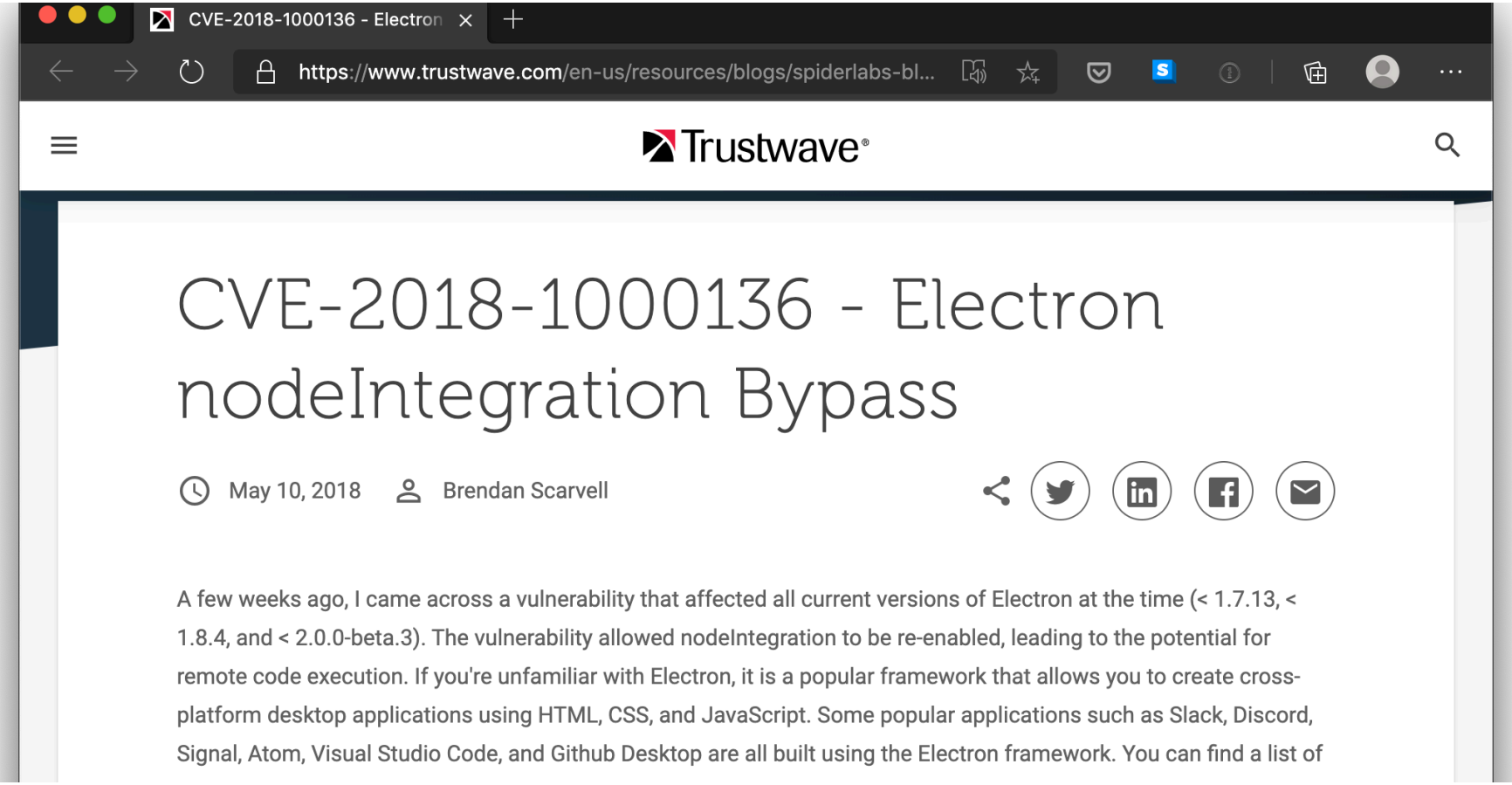
Visual Studio Code



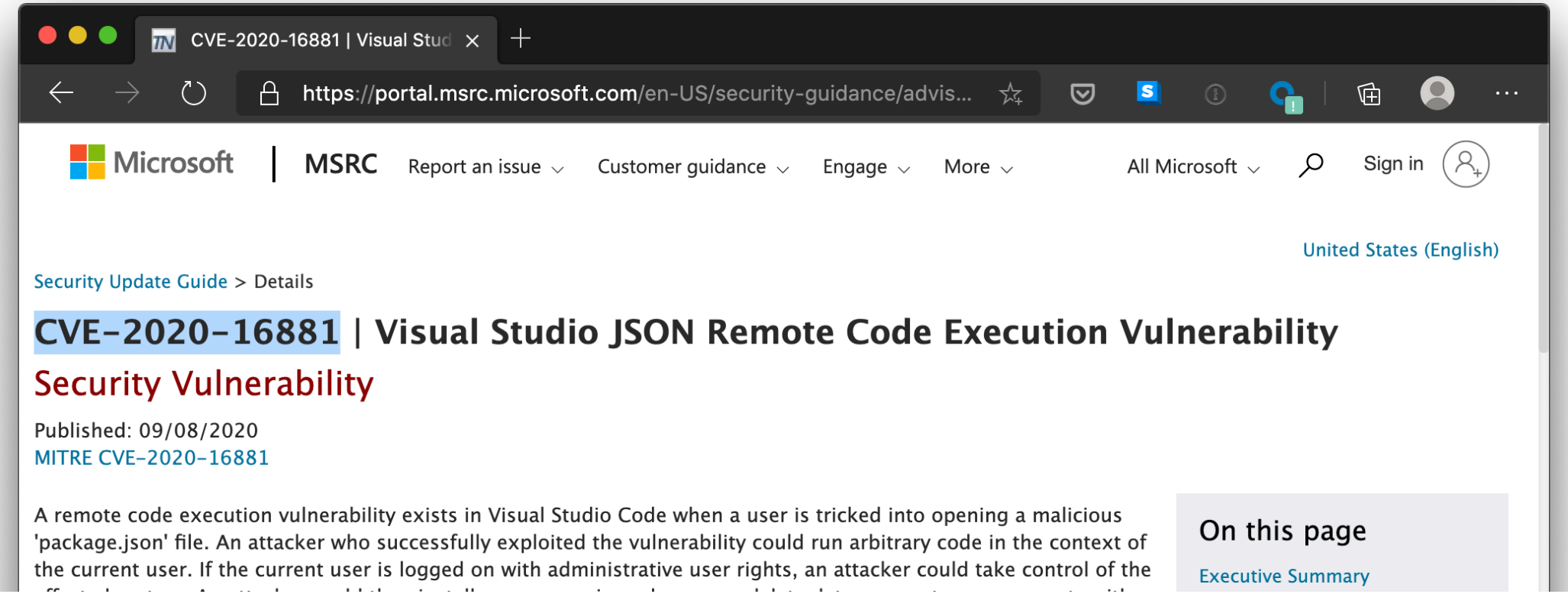
Visual Studio Code



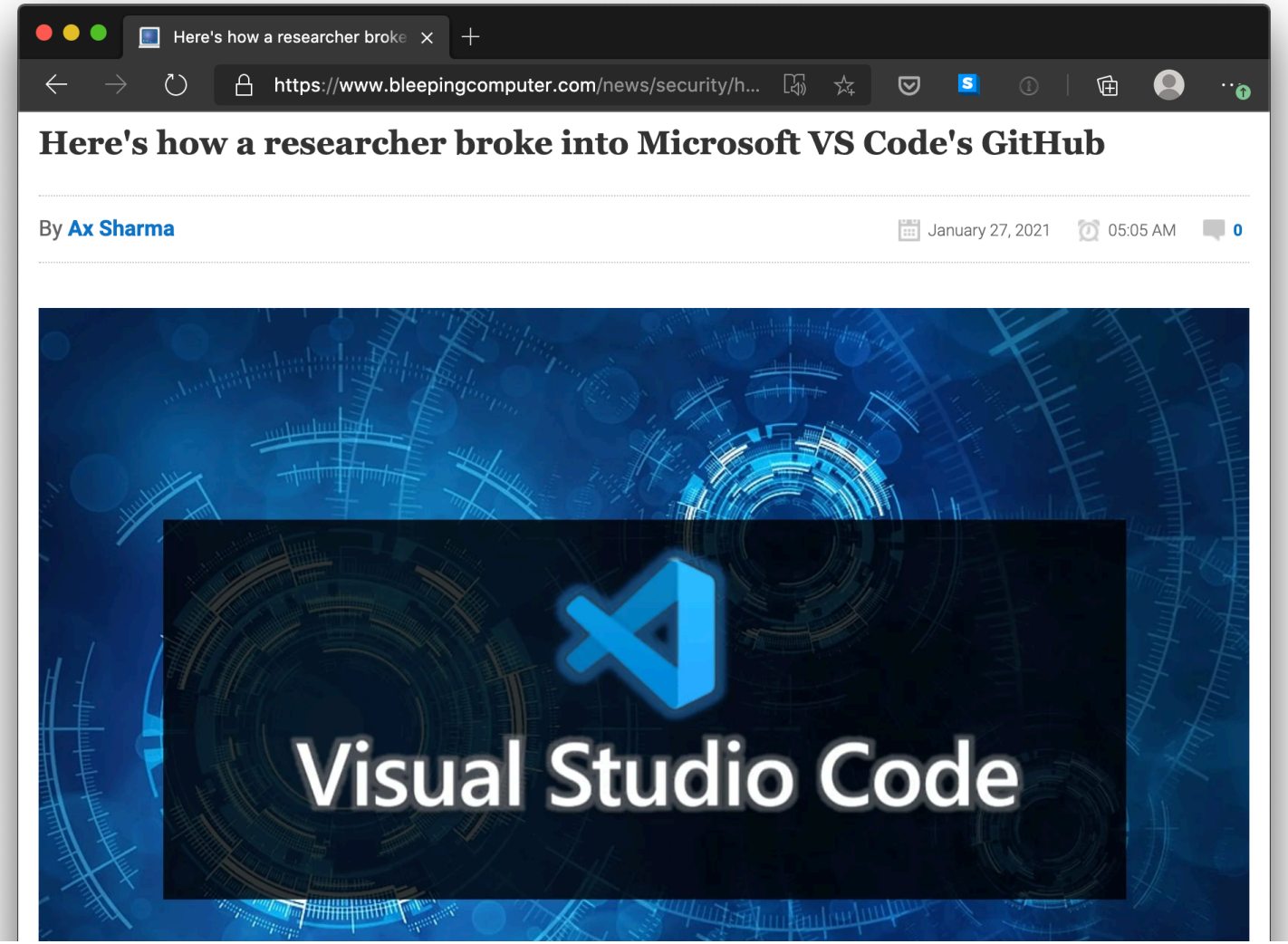
Visual Studio Code



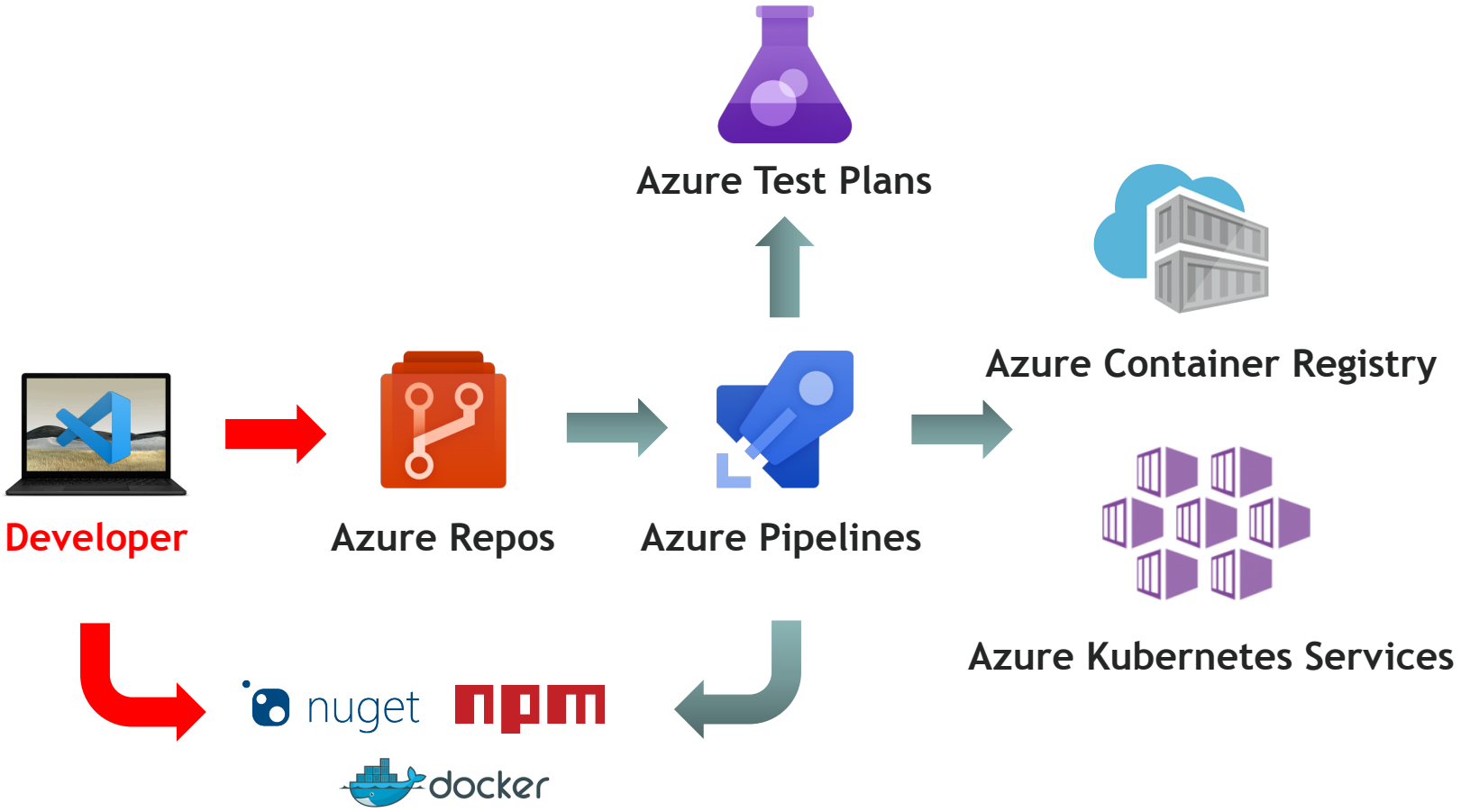
Visual Studio Code



Visual Studio Code



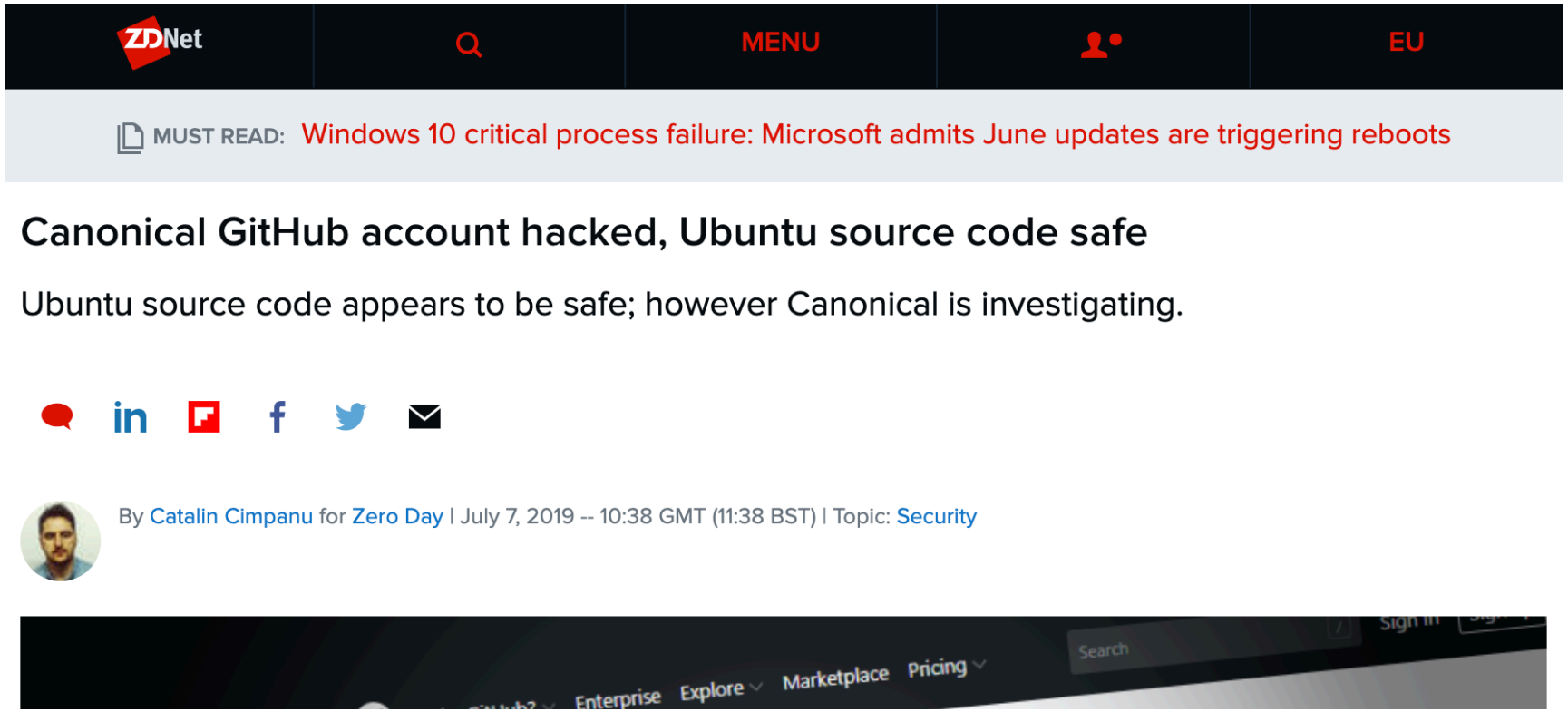
Software Supply Chain



Development Machine

- Package manager e.g. NuGet / NPM
- Transport-Layer Security (TLS)
    - Root Authority Trust
    - Downgrade, TLS 1.0 – 1.1 deprecated on NuGet
- Domain Name Service (DNS)
    - DNSSEC → NuGet.org and GitHub.com don’t support it

Canonical GitHub Account



Microsoft GitHub Account

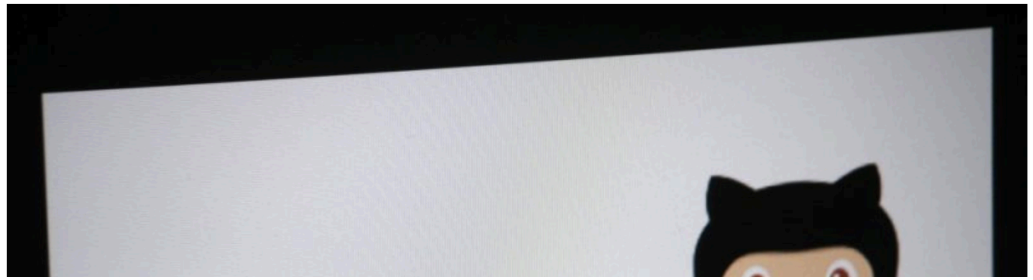
threatpost

Search

Podcast: Shifting Cloud Security Left With Infrastructure-as-C

Hackers Breach 3.5 Million MobiFriends Dating App Credentials

Report: Microsoft's GitHub Account Gets Hacked



INFOSEC INSIDER

Helping Remote Workers Overcome Remote Attacks

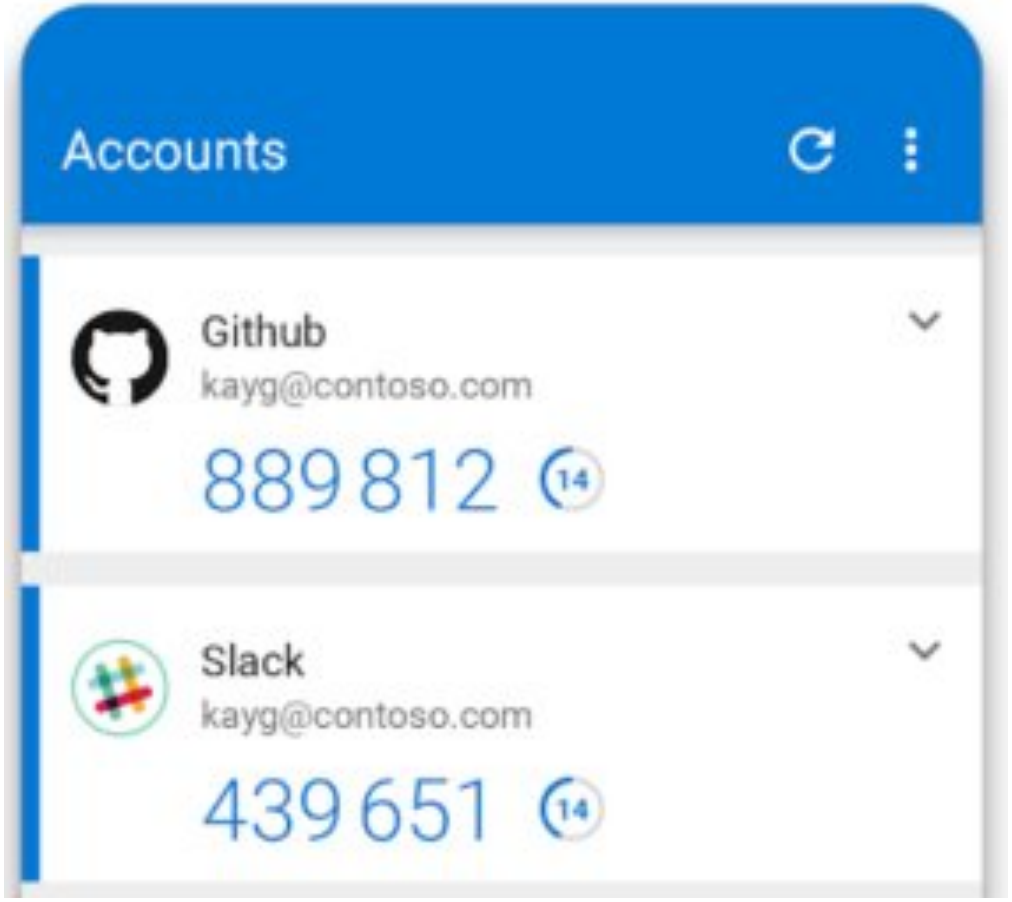
June 10, 2020 1

Understanding the Payload-Less Email Attacks Evading Your Security Team

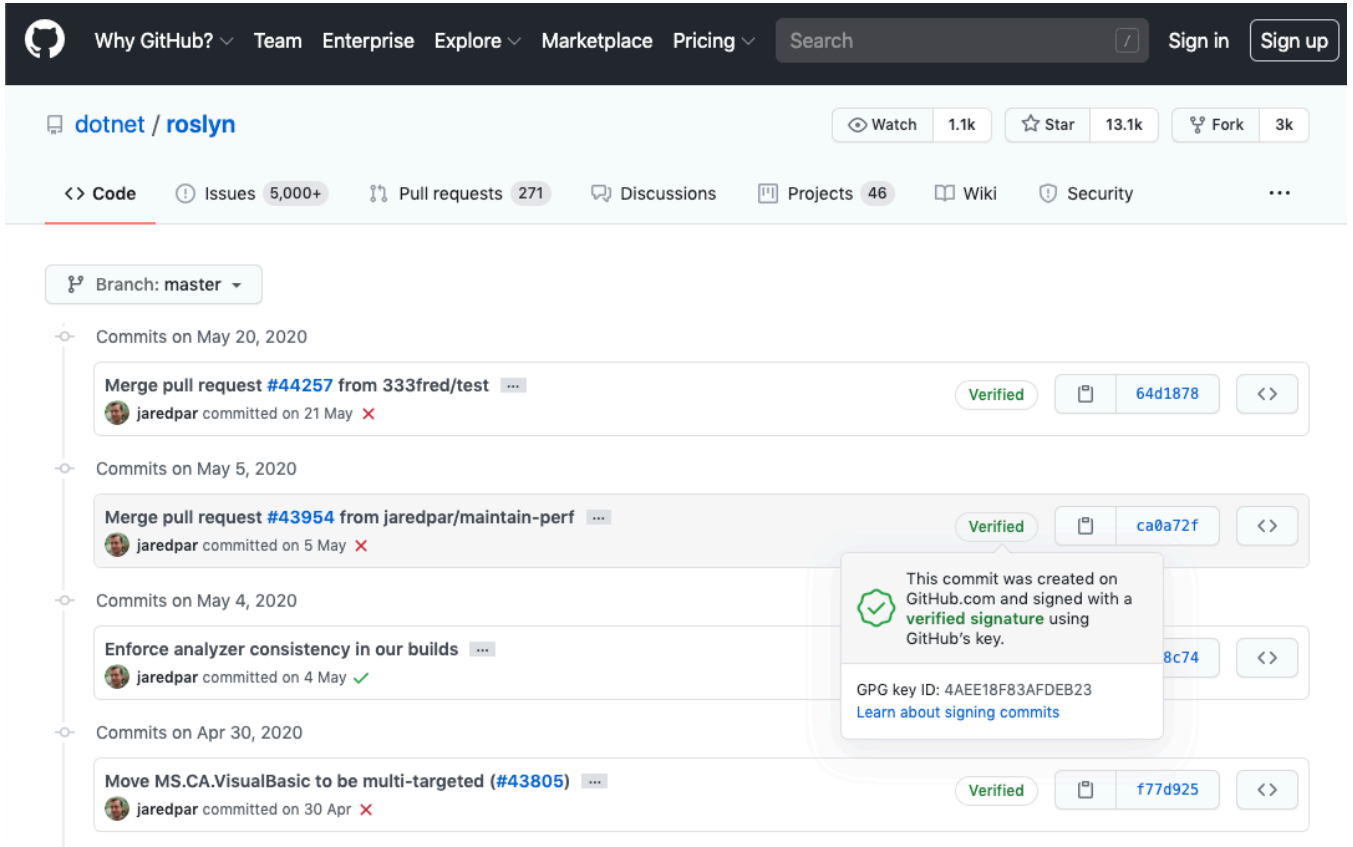
June 4, 2020

Long Tail Analysis: A New Hope in the Cybercrime Battle

Use MFA on source-repository

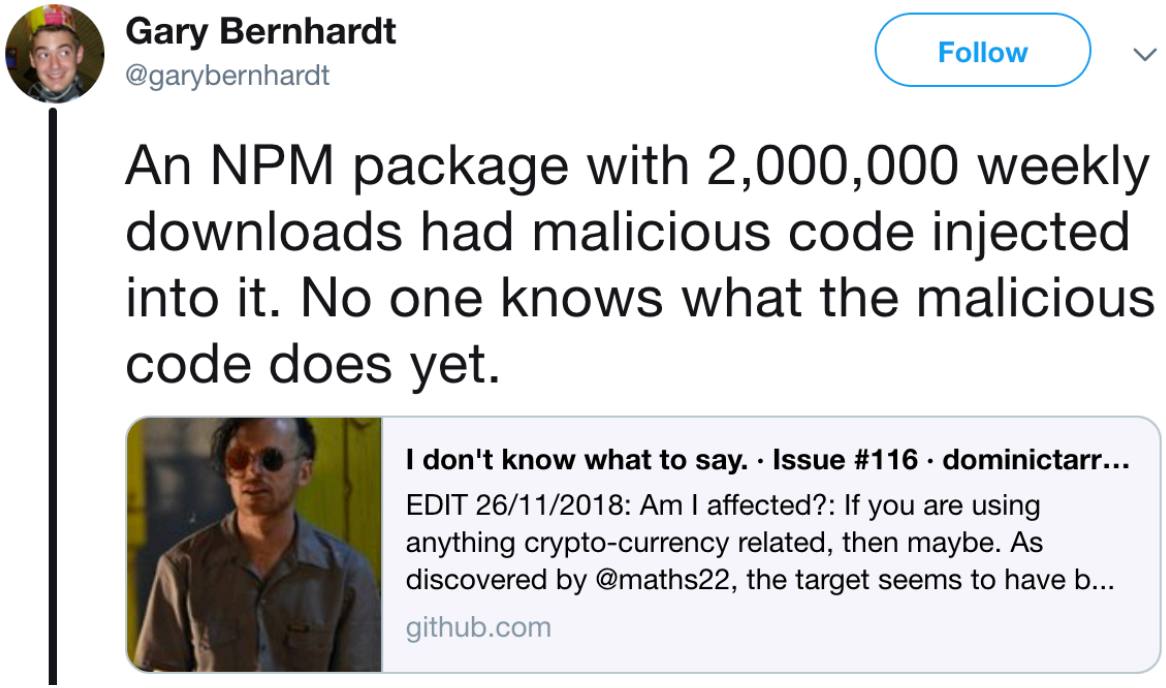


GIT Commit Signing

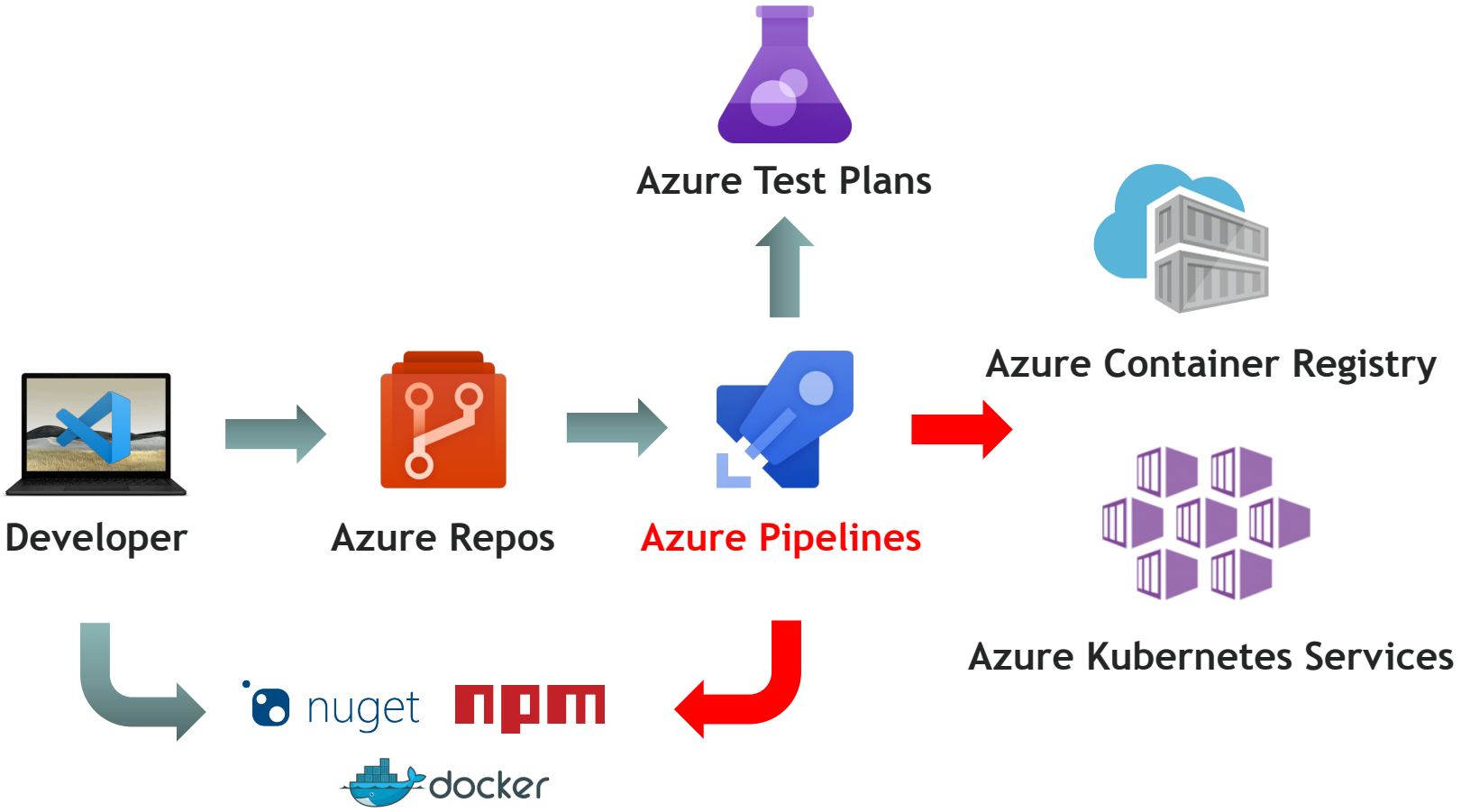


EvenStream NPM

- November 2018
- Is transitive dependency of 2000 other libraries



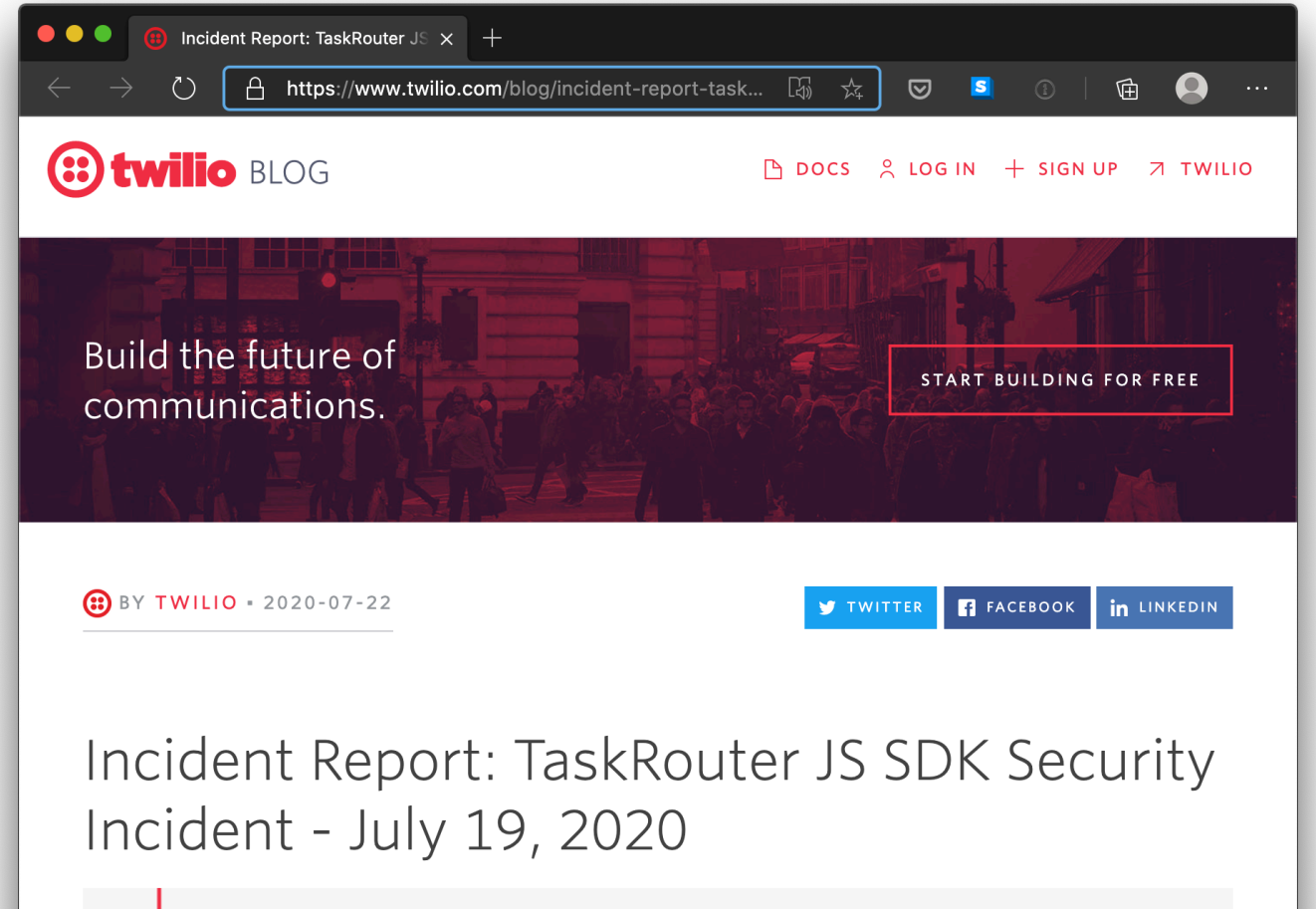
Software Supply Chain



Build / Deployment

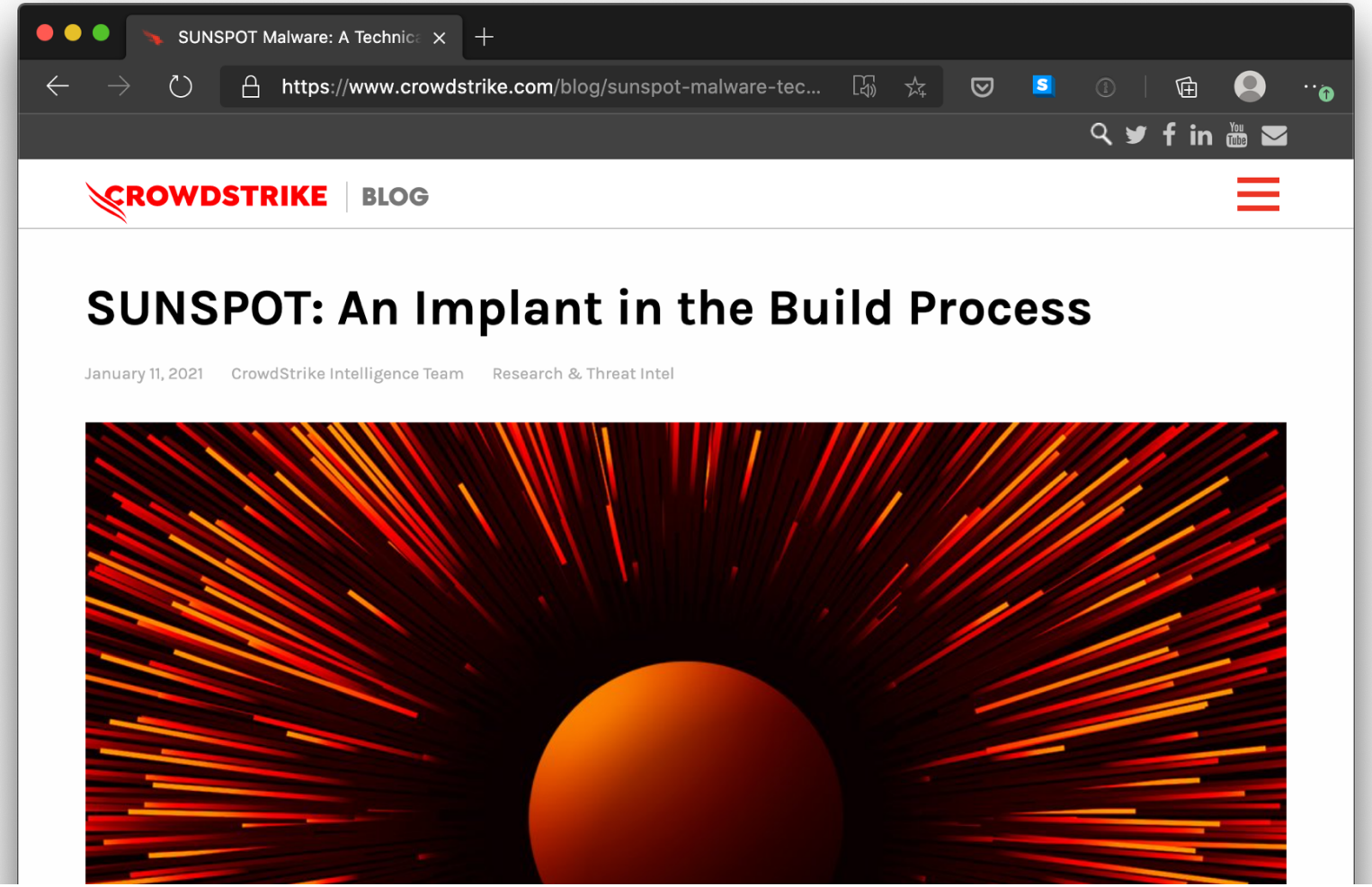
- What about hardware? Vendor trust?
- TLS issues?
- Compromised Docker Images
    - Two-Factor authentication in beta
- Build Server can be compromised

Twilio SDK

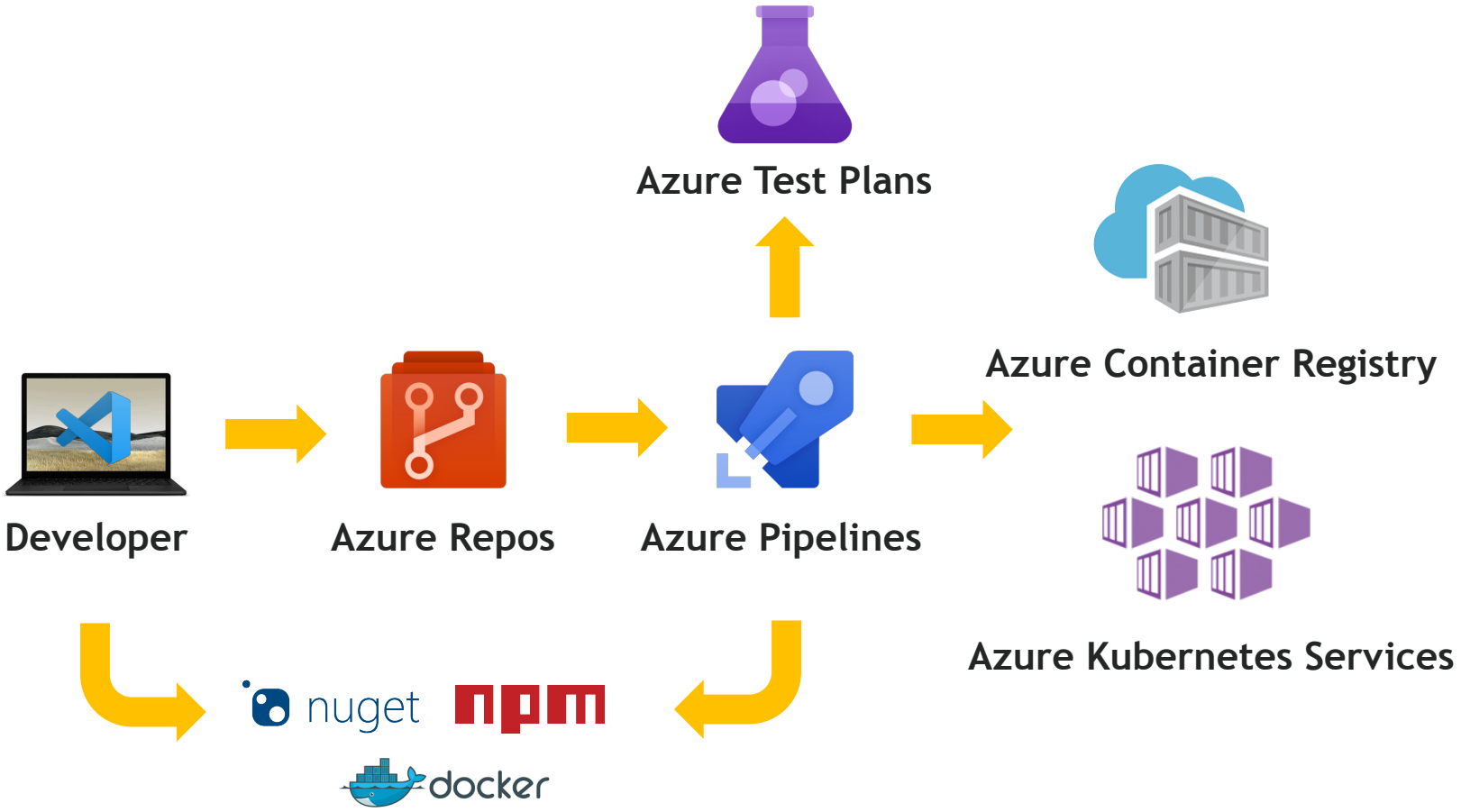

Incident Report: TaskRouter JS
https://www.twilio.com/blog/incident-report-task...
twilio BLOG
DOCS
LOG IN
SIGN UP
TWILIO
Build the future of communications.
START BUILDING FOR FREE
BY TWILIO • 2020-07-22
TWITTER
FACEBOOK
LINKEDIN
Incident Report: TaskRouter JS SDK Security Incident - July 19, 2020

Webmin Backdoor

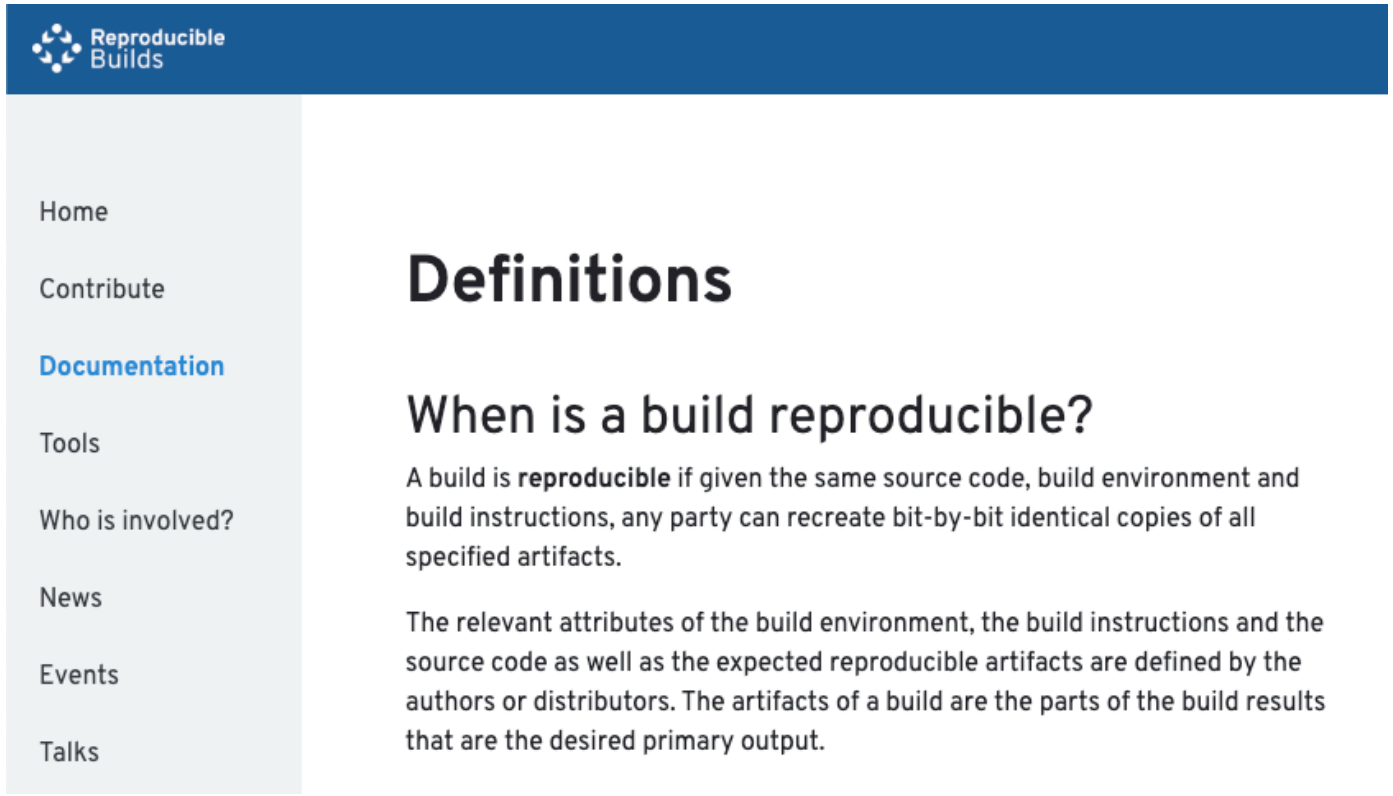
SolarWinds Sunspot



Software Supply Chain



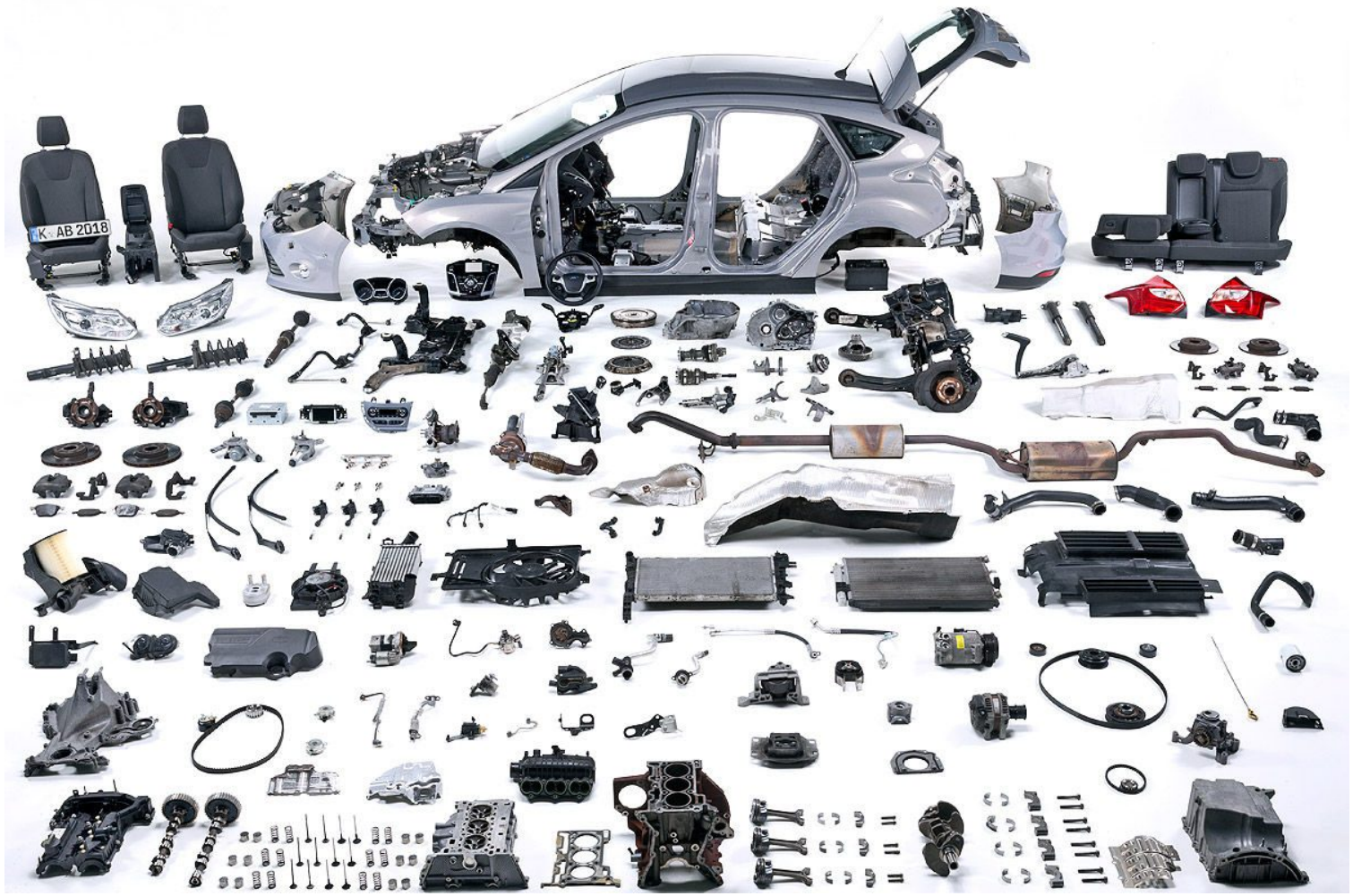
Reproducible/Deterministic Builds



Reproducable/Deterministic Builds

- Roslyn v1.1 started supporting some kind of determinism on how items are emitted
- Given same inputs, the compiled output will always be deterministic
- Inputs can be found in Roslyn compiler docs ‘Deterministic Inputs’

Automotive Industry



Car Supply Chain

Tata Steel Factory

- Iron Ore from Sweden
- ISO 6892-1 Tested/Certified
- Batch #1234

Bosch Factory

- Steel Batch #1234 Tata
- ECE-R90 Tested/Certified
- Serie #45678
- Used by Ford, Volkswagen and KIA

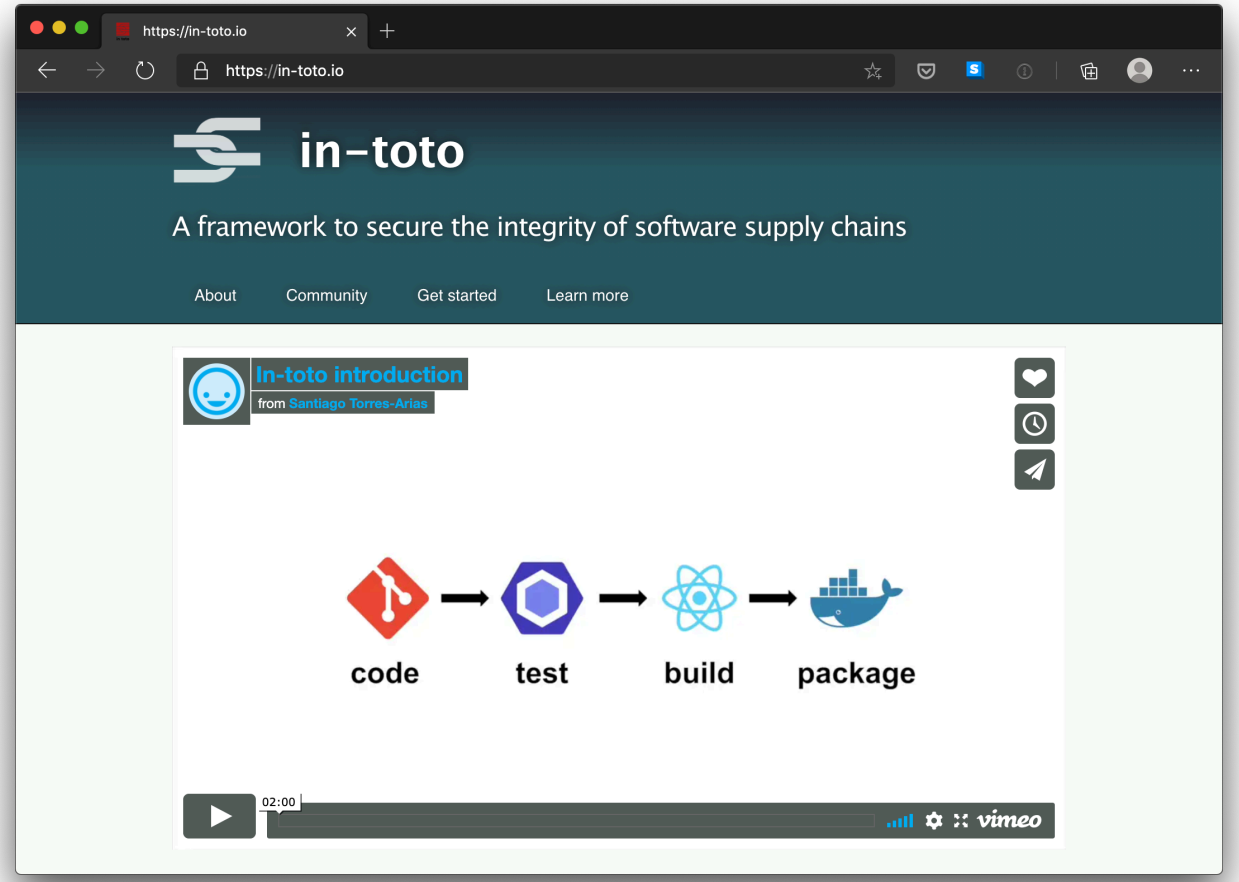
Ford Manufacturing

- Bosch Disk #45678
- Bosal Exhaust #RE9876
- Goodyear Tires #GY8877
- Focus VIN 1234567890

Software Bill of Materials (SBOM)

- Industry standard of describing the software
  - Producer Identity – Who Created it?
  - Product Identity – What's the product?
  - Integrity – Is the project unaltered?
  - Licensing – How can the project be used?
  - Creation – How was the product created? Process meets requirements?
  - Materials - How was the product created? Materials/Source used?
- CycloneDX – Lightweight SBOM with dependency graph
- NTIA.org - SBOM

In-toto



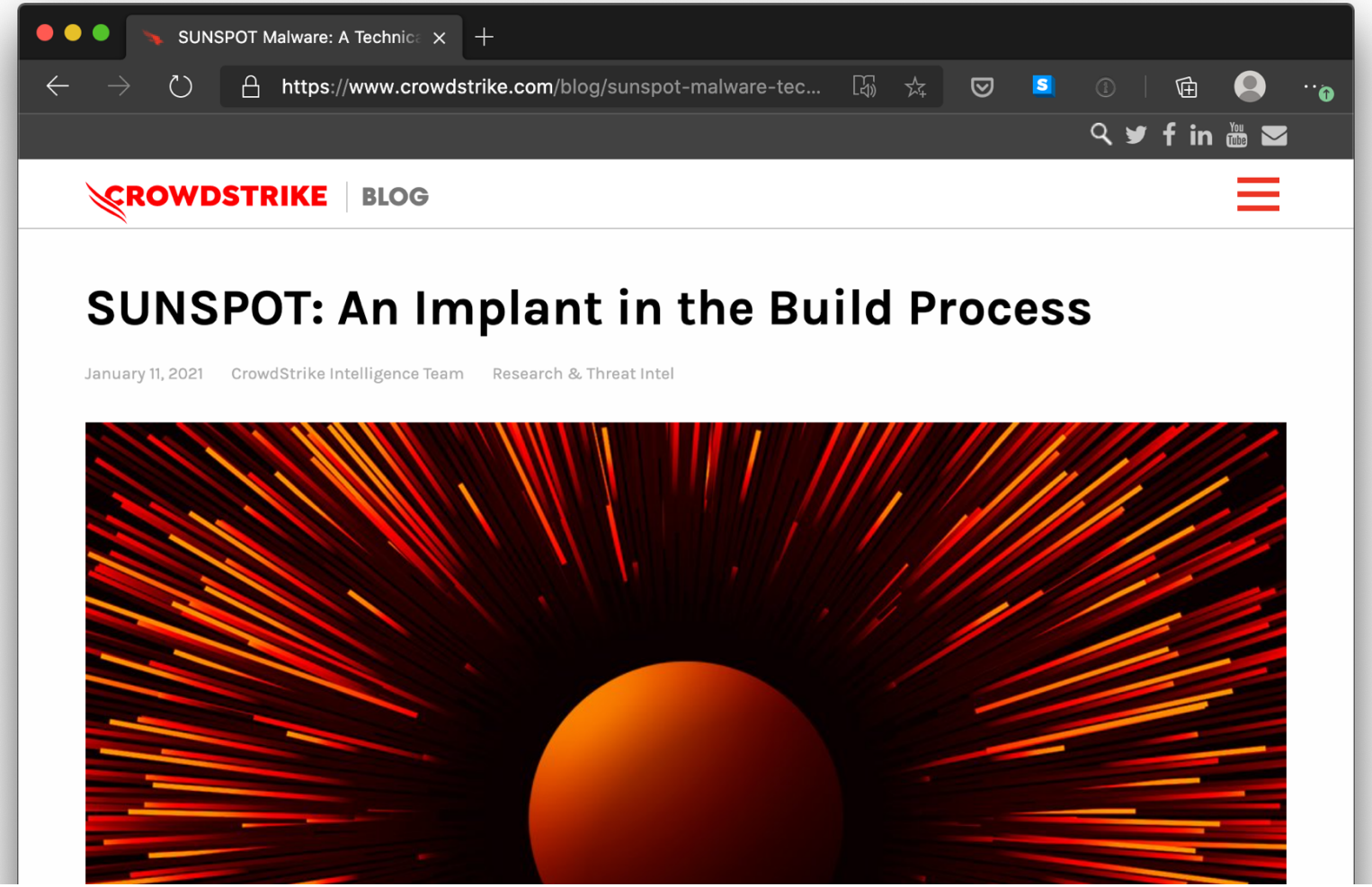
In-Toto – Demo - Terminology

- **Functionaries** that are identified by public key our supply chain.
  Niels (Project-Owner), Aimee (Developer) and Noud (Packager)

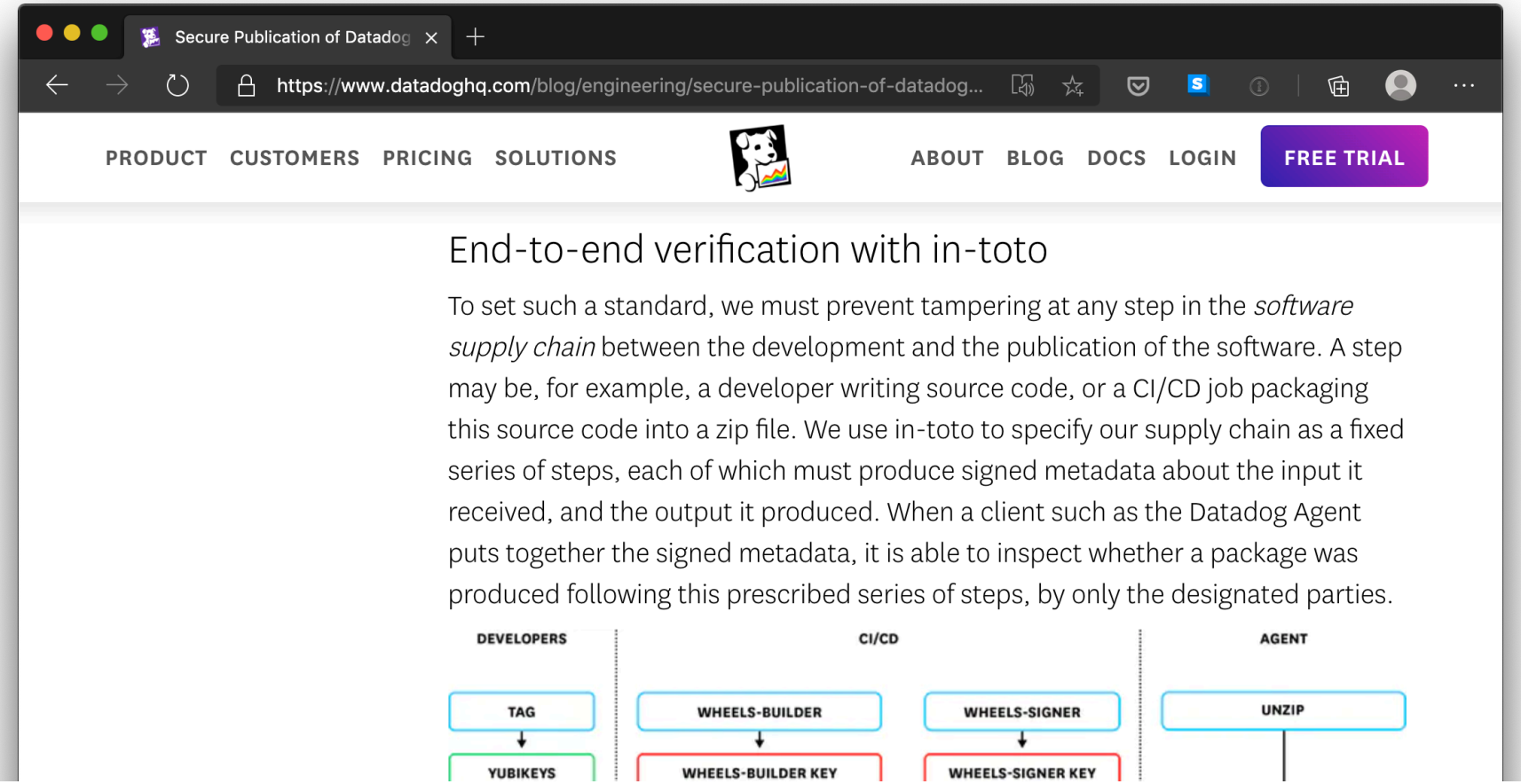
- **Project-Owner** defines a (**Supply Chain) Layout** that describes **what** happens and by **who** and what the produced **Materials** and **Byproducts** are.

- **Link** metadata is output of executed step in the **Layout**
  Materials are input, **Products** are output and can be used as **Materials** in later steps

SolarWinds Sunspot



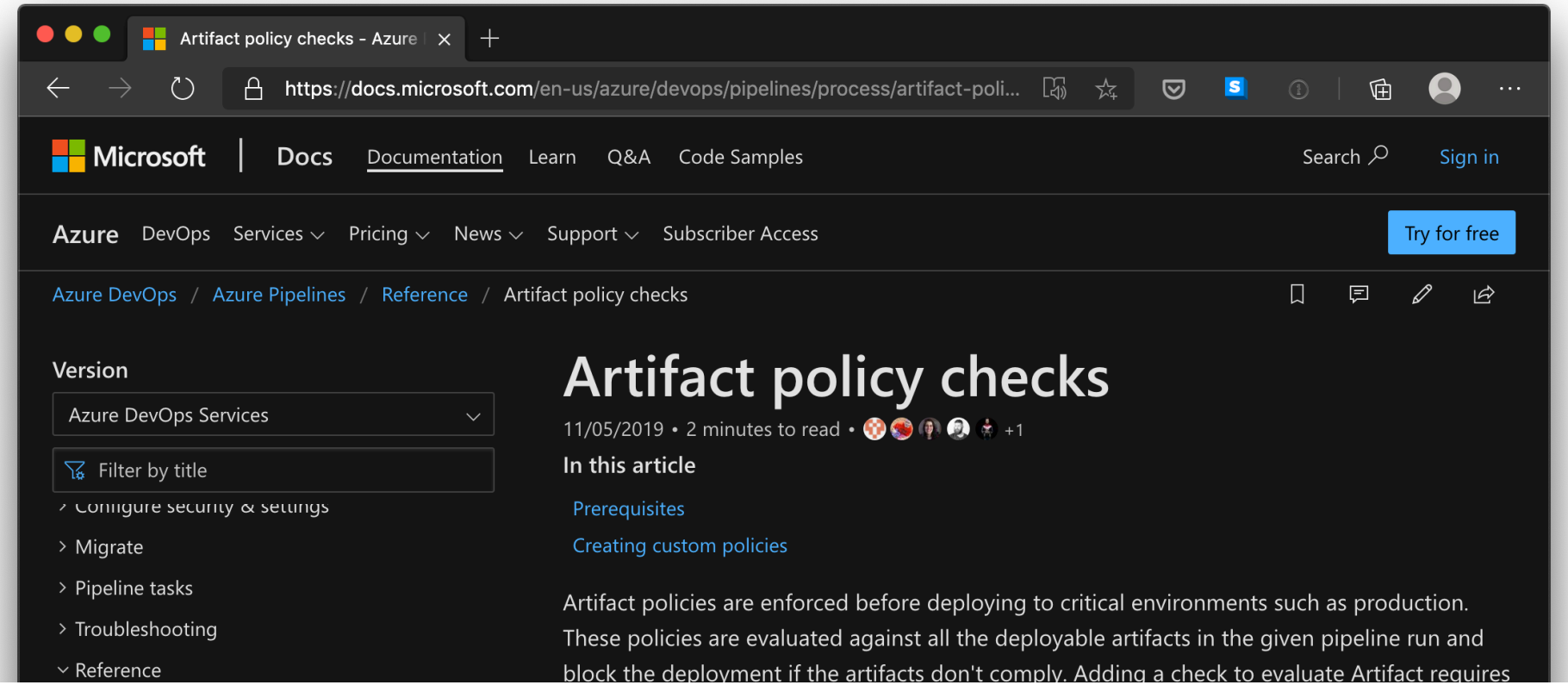
DataDog & In-Toto



Grafeas and Kritis by Google

- Grafeas – Component Metadata API
  - Container Analysis API on Google Cloud Platform
- Kritis – Deployment Authorization for Kubernetes Apps
  - Binary Authorization on Google Cloud Platform

Azure Pipelines Artifact Policy



Conclusion

- Be aware of your own (and other used) software supply chain(s).
- Know what you’re consuming and pulling into software projects.
- Use MFA on all accounts!
- Integrate security into your software lifecycle.
- Learn more on Software Bill of Materials (SBOM).

VERACODE

Thanks! Questions?

https://github.com/nielstanis/ndclondon2021

ntanis at veracode.com

@nielstanis on Twitter