Алексей Лукацкий
Бизнес-консультант по безопасности

pt

Мониторинг атак на|от подрядчиков

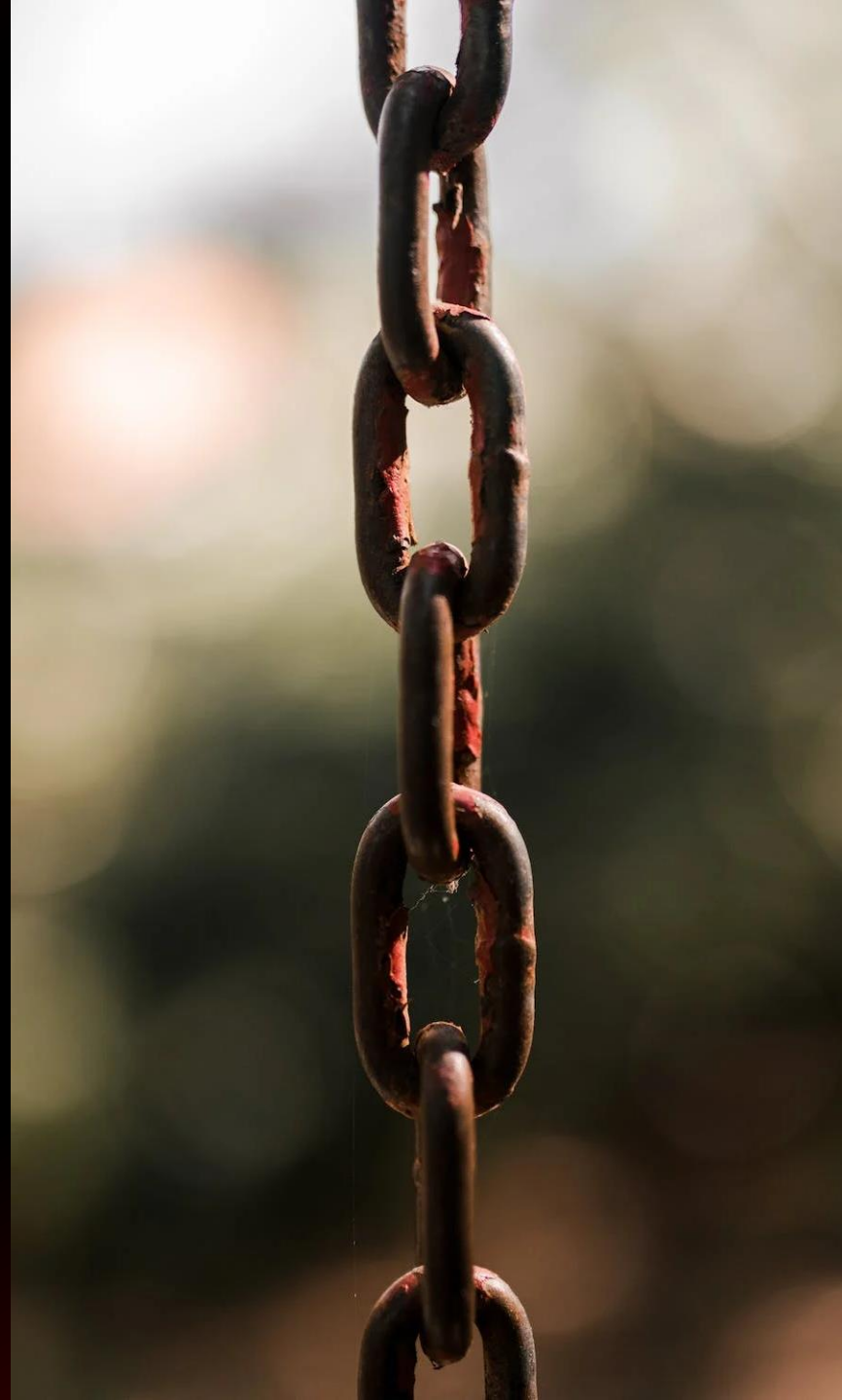
Что брать под контроль на примере реальных кейсов

Who am I?

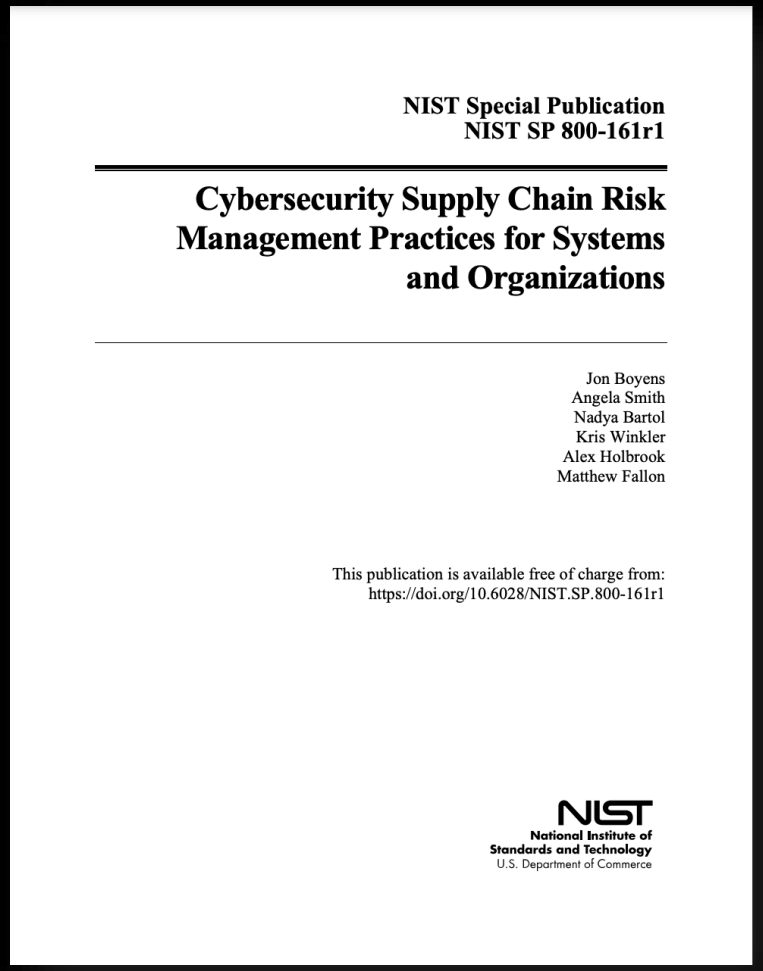
- Бизнес-консультант по безопасности в Positive Technologies
- Первый SOC строил в 1999-м в Украине
- Проектировал и аудировал SOCи в финансовом, энергетическом, нефтяном, телекоммуникационном, ИТ, государственном секторах, а также для спецслужб - в России, странах СНГ и Восточной Европы
- Участвовал в построении государственных CDC в странах СНГ

Защита цепочек поставок

- Управление защищенной конфигурацией ПО
- Предотвращение или обнаружение подмены критических компонентов
- «Безопасные» языки
- Безопасная разработка
- Supply Chain Red Teaming
- Доверенная доставка
- Усиленные механизмы доставки
- Трекинговые метки
- Контроль «родословной» по всей цепочке поставок
- Склад запчастей
- Множество поставщиков
- Доверенные поставщики
- Анонимность закупки
- Термальный и электромагнитный анализ
- Ограничение сетевого трафика
- Визуальная инспекция
- Криптография
- Видимость цепочки поставки
- Доверие к персоналу
- Безопасность обновлений ПО
- ...



Что в целом говорит нормативка?



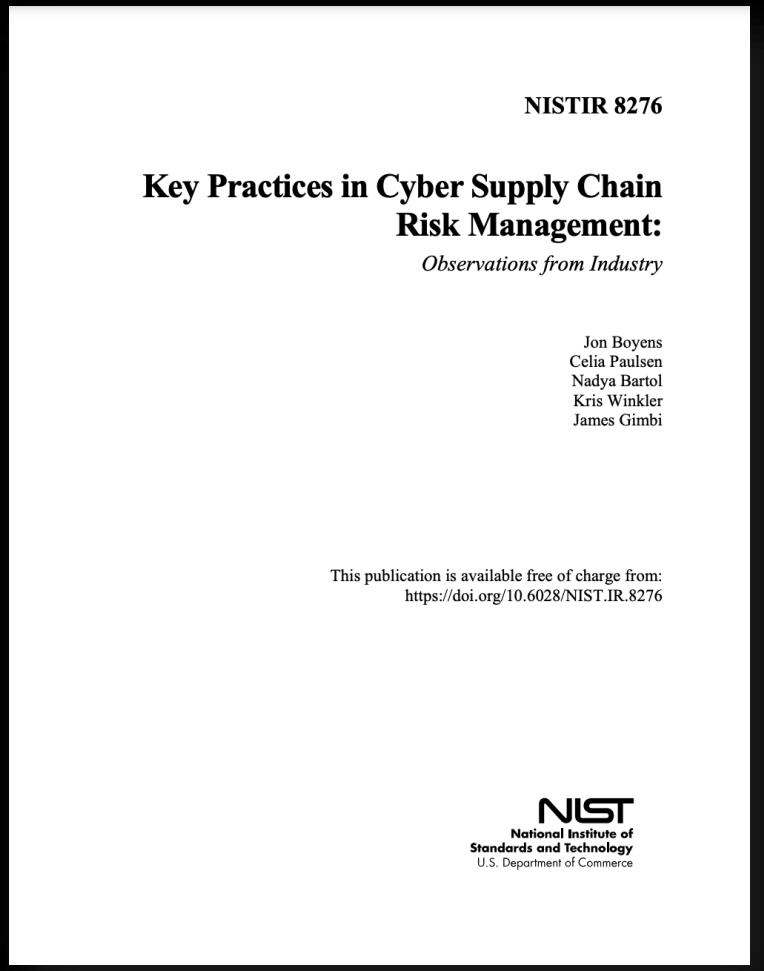
NIST Special Publication
NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



NISTIR 8276

Key Practices in Cyber Supply Chain Risk Management:

Observations from Industry

Jon Boyens
Celia Paulsen
Nadya Bartol
Kris Winkler
James Gimbi

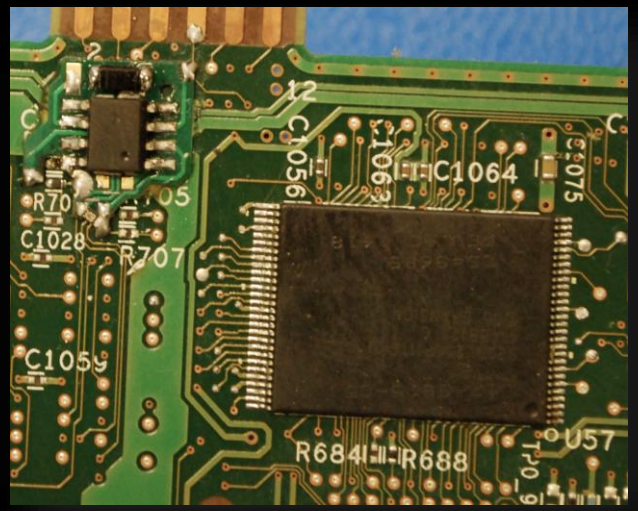
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8276

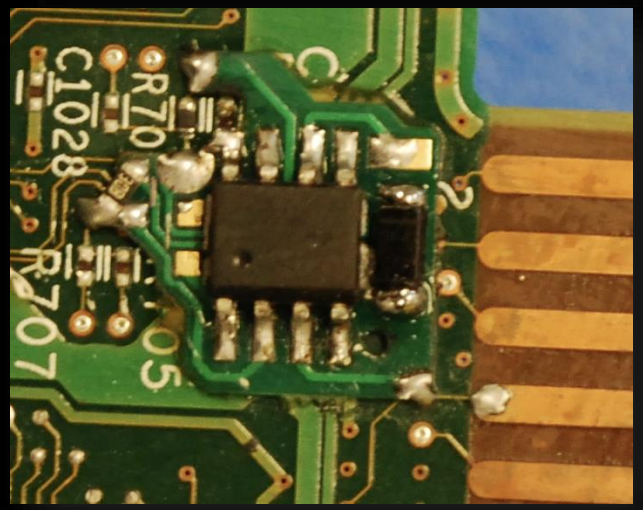
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Угрозы от подрядчиков

- Внедрение программных закладок
- Подмена программных компонентов
- Компрометация системы удаленного управления
- Компрометация сайтов подрядчиков
- Аппаратные импланты
- Подмена аппаратных компонентов
- НСД со стороны сотрудников подрядчика

Не все можно легко обнаружить
Аппаратные импланты





- Установка дополнительного чипа и микроконтроллера на плате маршрутизатора Cisco
  - Выполнение расширенного функционала
- Внедрение вредоносного ПО в память маршрутизатора
  - Обход лицензионных проверок
  - Возможность работы дополнительного чипа

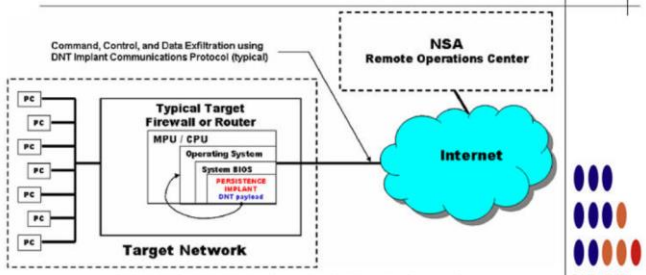
Какова ваша модель нарушителя?

TOP SECRET//COMINT//REL TO USA, FVEY

JETPLOW
ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08



(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been widely deployed. Current availability restricted based on OS version (inquire for details). **Unit Cost:** $0

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

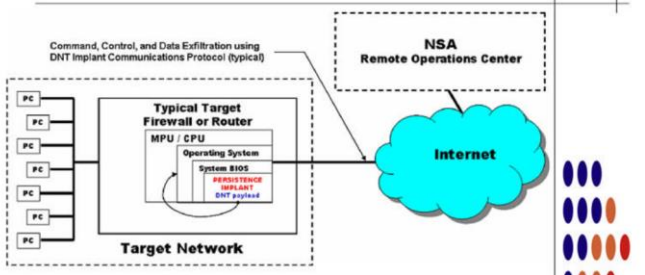
TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

HEADWATER
ANT Product Data

(TS//SI//REL) HEADWATER is a Persistent Backdoor (PBD) software implant for selected Huawei routers. The implant will enable covert functions to be remotely executed within the router via an Internet connection.

06/24/08



(TS//SI//REL) HEADWATER Persistence Implant Concept of Operations

(TS//SI//REL) HEADWATER PBD implant will be transferred remotely over the Internet to the selected target router by Remote Operations Center (ROC) personnel. After the transfer process is complete, the PBD will be installed in the router's boot ROM via an upgrade command. The PBD will then be activated after a system reboot. Once activated, the ROC operators will be able to use DNT's HAMMERMILL Insertion Tool (HIT) to control the PBD as it captures and examines all IP packets passing through the host router.

(TS//SI//REL) HEADWATER is the cover term for the PBD for Huawei Technologies routers. PBD has been adopted for use in the joint NSA/CIA effort to exploit Huawei network equipment. (The cover name for this joint project is TURBOPANDA.)

Status: (U//FOUO) On the shelf ready for deployment.

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//NOFORN

June 2010

SID today

(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By: (U//FOUO) [redacted], Chief, Access and Target Development (S3261)

(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away… In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

(TS//SI//NF) In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network. Upon initiating the survey, SIGINT analysts from TAO/Requirements & Targeting determined that the implanted device was providing even greater accesses than we had hoped: We knew the devices were bound for the Syrian Telecommunications Establishment (STE) to be used as part of their internet backbone, but what we did not know was that STE's GSM (cellular)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20350501

TOP SECRET//COMINT//NOFORN

Знай своего подрядчика

- Поставщики ПО и железа
- Разработчики используемых библиотек и компонентов
- Хостинг-провайдеры
- Провайдеры MSP / MSSP / MDR / SOC
- ИТ/ОТ-интеграторы
- Подрядчики (К+...)
- ...

Смотрите на всю цепочку

Процедура производства и поставки оборудования (пример)

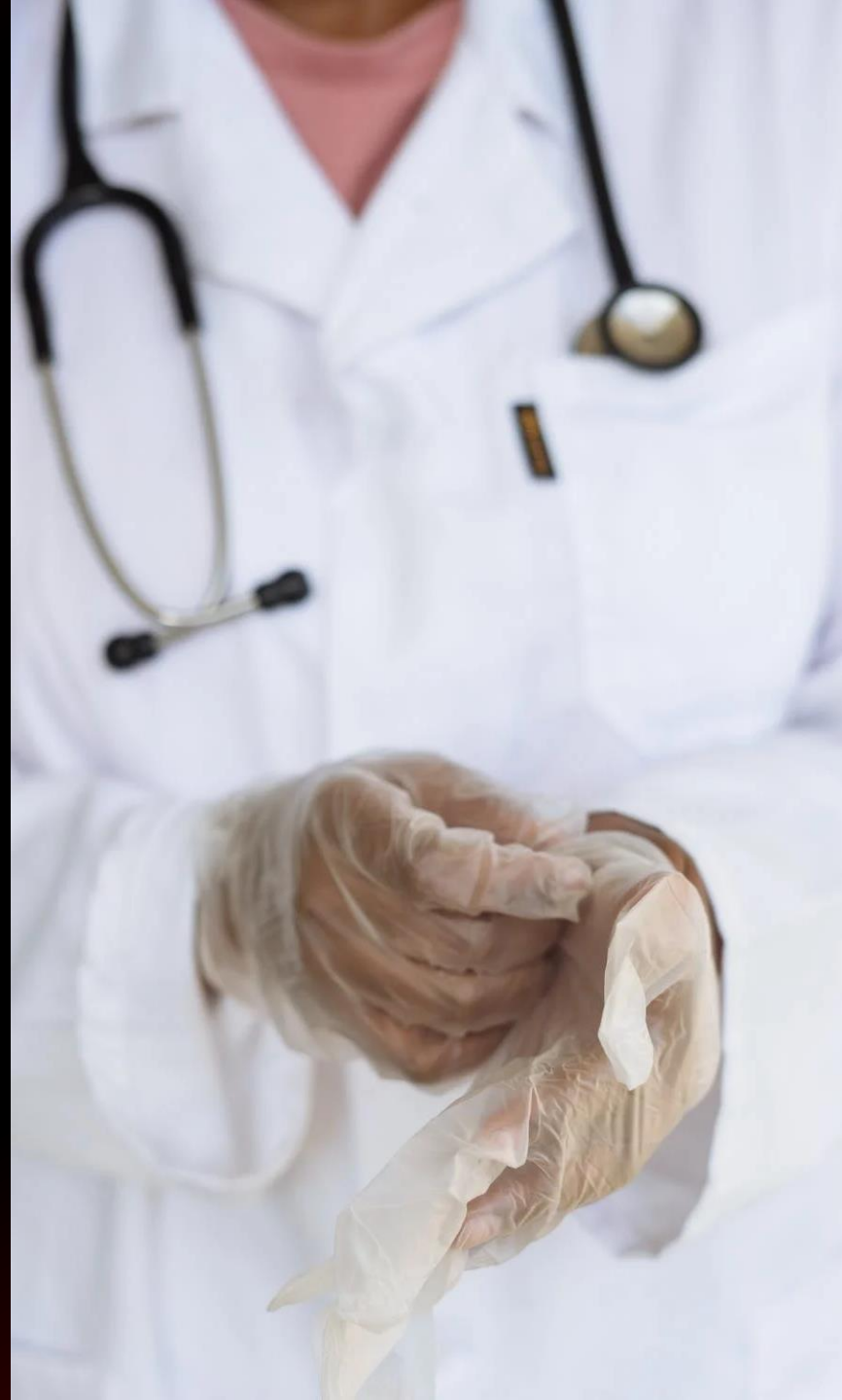
Приоритизируйте

- Размер дохода
- Доступ к важным/ценным данным
- Объем данных и число узлов, к которым подрядчик имеет доступ
- Может ли подрядчик стать причиной вашей компрометации?
- Попробуйте Impact Analysis Tool for Interdependent Cyber Supply Chain Risks

https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8272.pdf

Оценка площади атаки

- Инвентаризация всех своих активов
- Регулярное сканирование открытых портов и трендовых уязвимостей на периметре подрядчиков (согласно договора)
- Что делать с субподрядчиками?

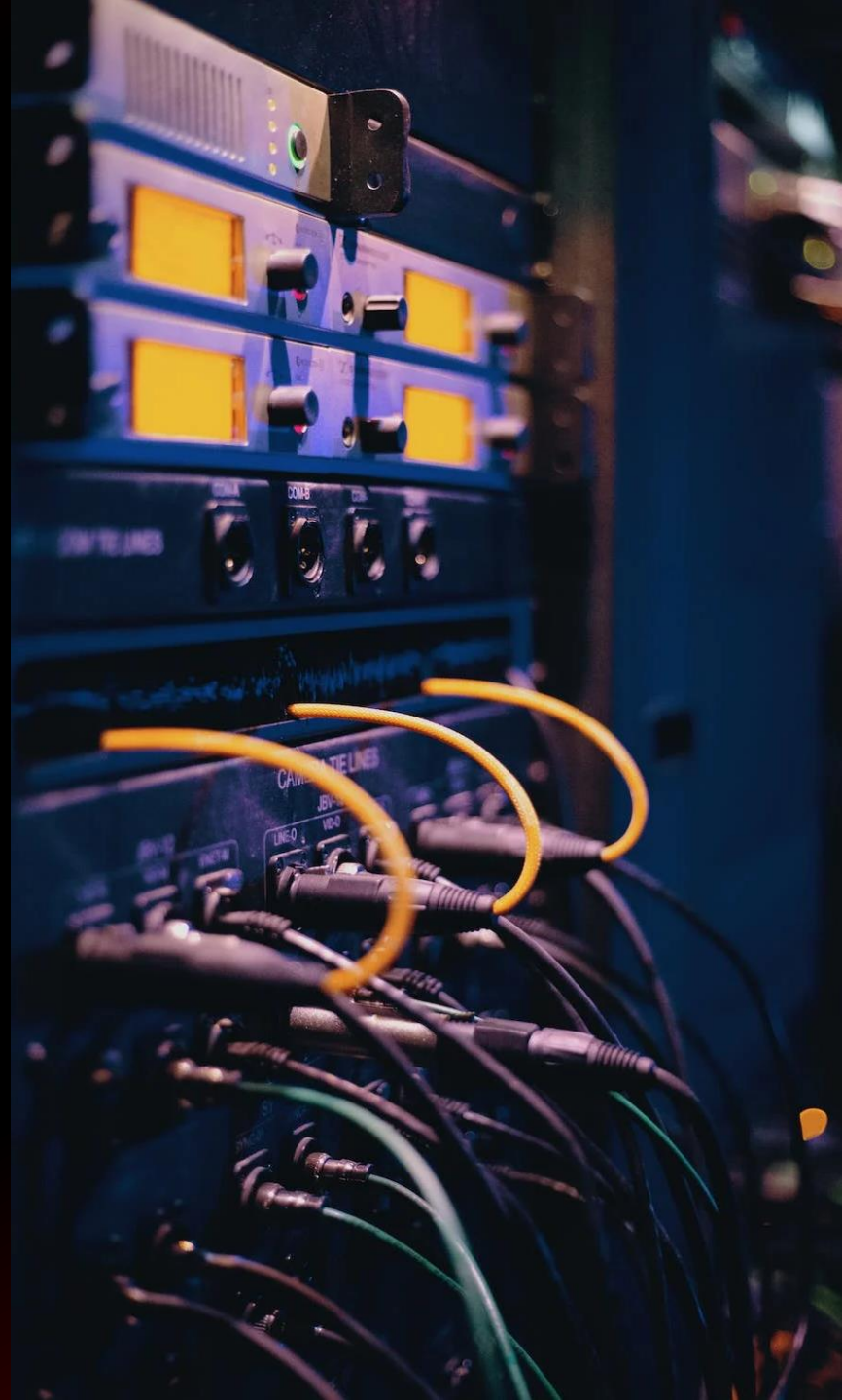


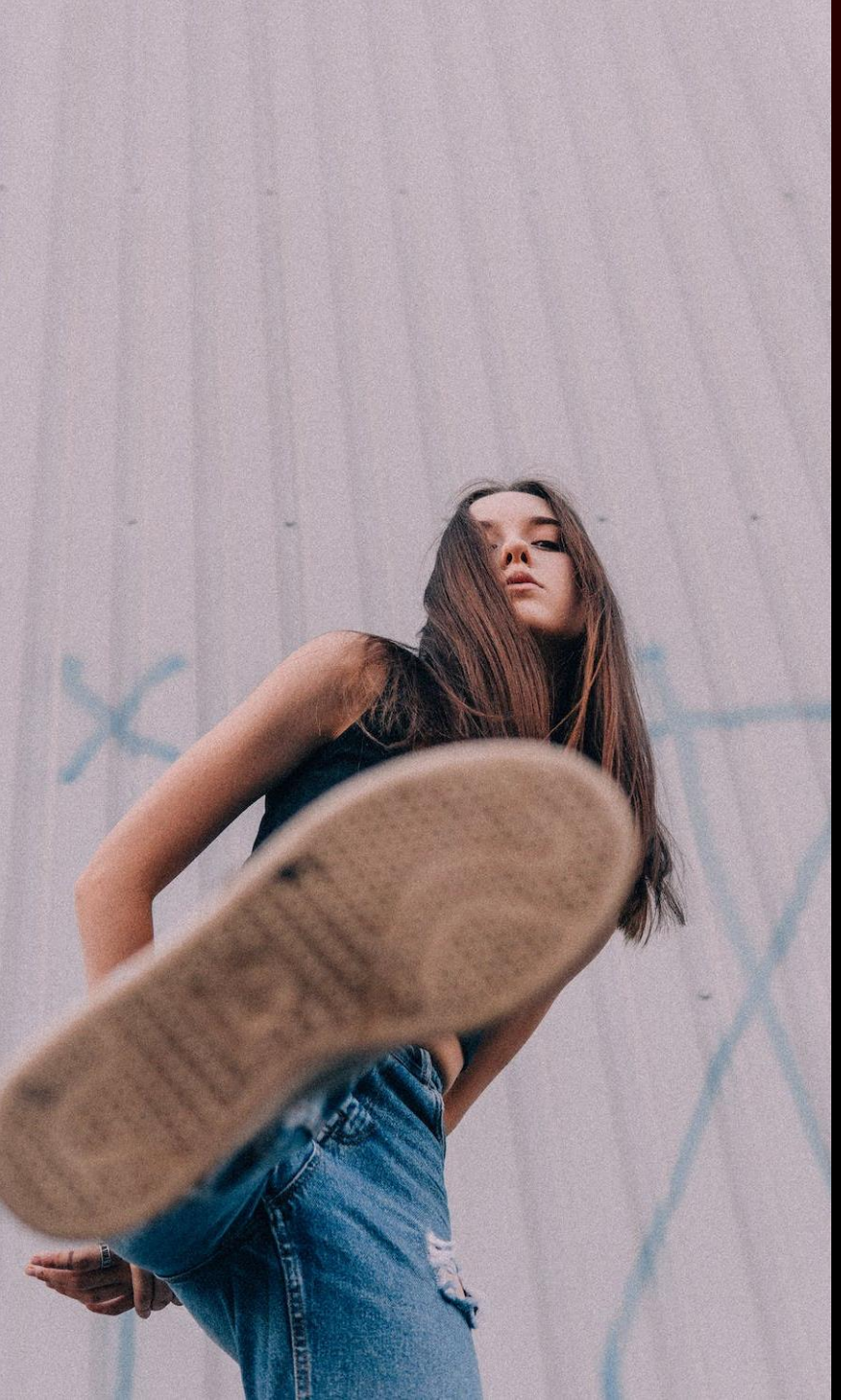
Индикаторы

- Файловые (хеши и имена файлов)
- Сетевые (IP, имена доменов)
- Поведенческие (нетипичный трафик или системная активность)
- Артефакты (ключи реестра, конфиги, сертификаты)

Сетевые индикаторы

- Нетипичный трафик в сторону подрядчика
- Превышение типичного объема данных
- ПО подрядчика коммуницирует с известными C2-серверами или нетипичными IP / доменами / геолокациями
- Сканирование со стороны подрядчика



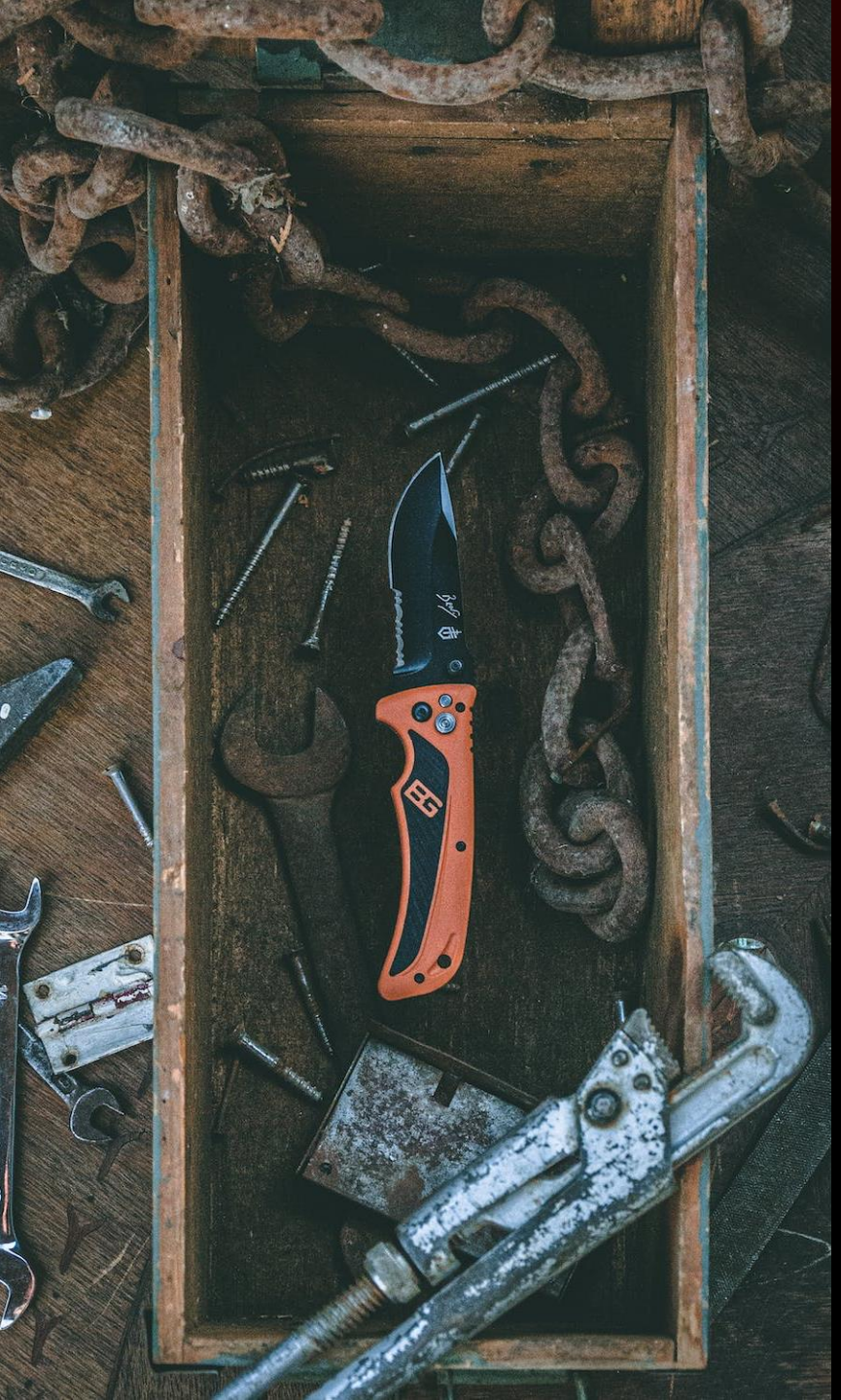


Поведенческие индикаторы

- Доступ к нетипичным узлам или данным в инфраструктуре
- Повышение привилегий
- Доступ в нетипичное время
- Неудачные попытки аутентификации
- Нетипичные места входа

Файловые индикаторы

- Несоответствие хеша скачанного / полученного файла эталонному
- Неизвестные ранее файлы



Что типично для подрядчика?!

Что является предметом договора?

Каталог шаблонов атак

Attack Identifier: A3

Target (Attack Type): Hardware: Firmware:

Software: Yes

Description (Attack Act): System is compromised by the components during development or update.

Attack Vector: Adversary with access to software proce environment or software support activity update enviro

Attack Origin: Staff within the software engineering en

Attack Goal: Disruption: Yes

Corruption: Yes

Attack Impact: System may function in a manner that i

References: Based on NIST SP 800-30; page E-4

Threat: An adversary with access to software processes software support environment can insert malicious soft development or update/maintenance.

Vulnerabilities: The development environment or softv susceptible To an adversary inserting malicious softwar or update.

Attack Points: Program Office:

Prime Contractor: Yes

Sub-Contractor: Yes

Integrator Facility: Yes

Applicable Life Cycle Phases: Ma Te

Engineering and Manufactur

Production

Opera

Шаблон атаки (один из 41)

Attack ID	Program Office	Prime Contractor	Sub-Contractor	Integrator Facility	SW Developer	HW Developer	SC Physical Flow	SC Info/Data Flow
A14	■							
A7	■	■						
A30	■	■						■
A37	■	■						■
A36	■	■		■				■
A28	■					■		
A16	■							■
A17	■							■
A13		■	■		■			
A18		■	■		■			
A3		■	■	■	■			
A4		■	■	■	■			
A40		■	■	■	■			
A41		■	■	■		■		
A20		■	■	■	■			■
A21		■	■	■	■			■
A38		■	■	■	■			■
A39		■	■	■	■			■
A12		■	■	■	■	■	■	
A1		■	■	■	■		■	■
A8			■	■		■		
A9			■	■		■		
A23				■				
A19				■	■			
A26				■	■			
A32				■	■			
A10				■		■		
A25				■		■		
A5				■		■	■	
A29				■		■	■	
A31				■		■		■
A35					■		■	■
A6						■		
A22						■		
A24						■		
A33						■	■	
A34						■		
A2							■	
A11							■	
A15							■	
A27								■

Применимость атак

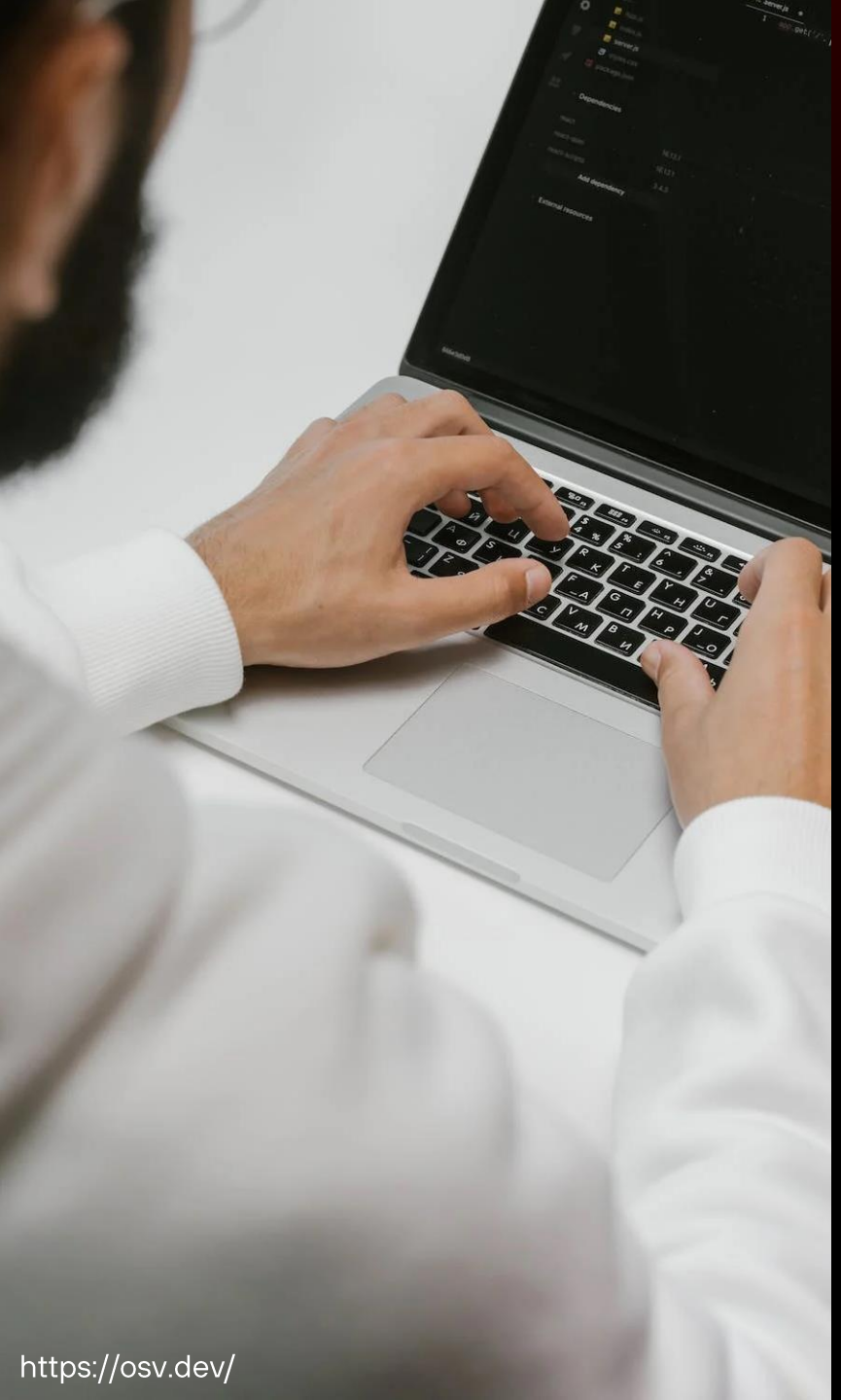
https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf

Threat Intelligence

- Мониторинг источников TI с информацией об угрозах на подрядчиков

Organization	Breach Date	Adversary	Source
Boeing	November 2023	LockBit	cisa.gov / (archived)
BeyondTrust	October 2023	Unknown	beyondtrust.com / (archived)
Okta	October 2023	Unknown	sec.okta.com / (archived)
BHI Energy	October 2023	Akira	documentcloud.org / (archived)
D-Link	October 2023	"succumb"	dlink.com / (archived)
Kroll	August 2023	Unknown	kroll.com / (archived)
Microsoft	July 2023	Storm-0558 (CN MSS)	microsoft.com / (archived)
JumpCloud	July 2023	UNC4899 (DPRK RGB)	jumpcloud.com / (archived)
Dragos	May 2023	"KyivWarrior"	dragos.com / (archived)
3CX	March 2023	UNC4736 (DPRK RGB)	mandiant.com / (archived)
Coinbase	February 2023	0ktapus (suspected)	coinbase.com / (archived)
Reddit	February 2023	0ktapus (suspected)	reddit.com / (archived)
CircleCI	January 2023	Unknown	circleci.com / (archived)
LastPass	October 2022	Unknown	blog.lastpass.com / (archived)
Uber	September 2022	Lapsus$ (suspected)	uber.com / (archived)
Okta	August 2022	0ktapus	sec.okta.com / (archived)

https://github.com/BushidoUK/Breach-Report-Collection



Базы данных уязвимостей

- Мониторинг известных уязвимостей в open source с помощью сканеров или фидов

Command Line Tools (OSV-Scanner)

Install OSV-Scanner

```
go install github.com/google/osv-scanner/cmd/osv-scanner@v1
```

Scan SBOM or Lockfiles

```
osv-scanner --sbom=cycloned-or-spdx-sbom.json
osv-scanner --lockfile=package-lock.json
```

Scan directory recursively

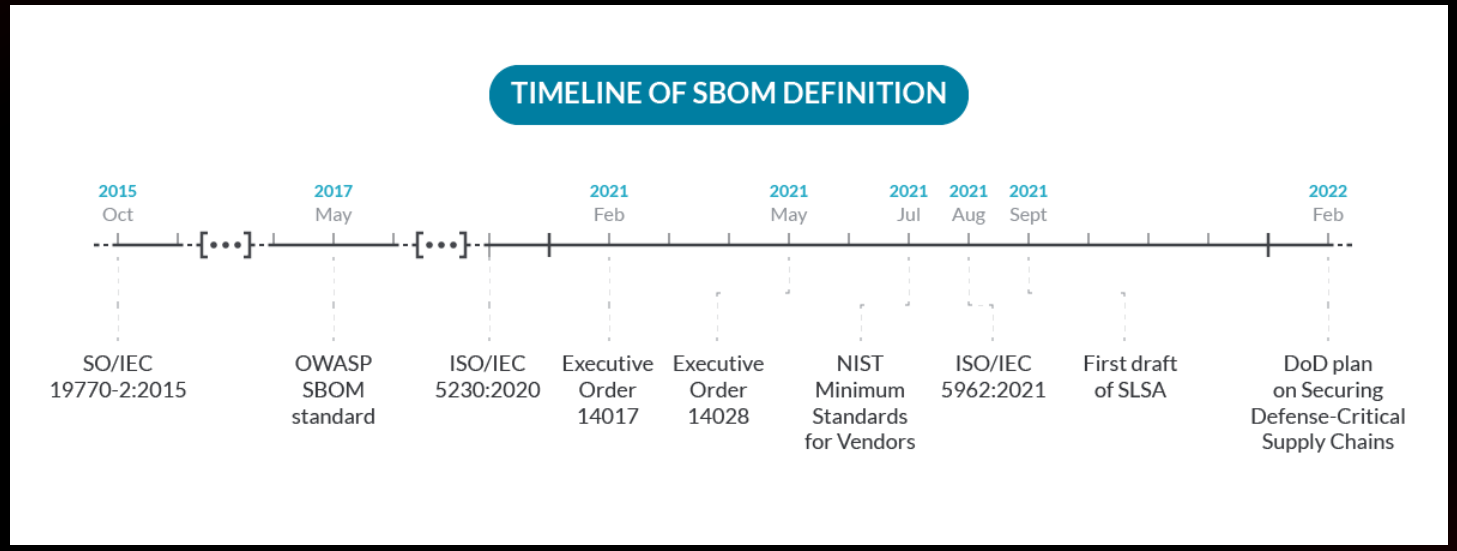
```
osv-scanner -r path/to/your/project
```

More details

https://osv.dev/

Software Bill of Material

- Список всех зависимостей, файлов, лицензий и других компонентов ПО

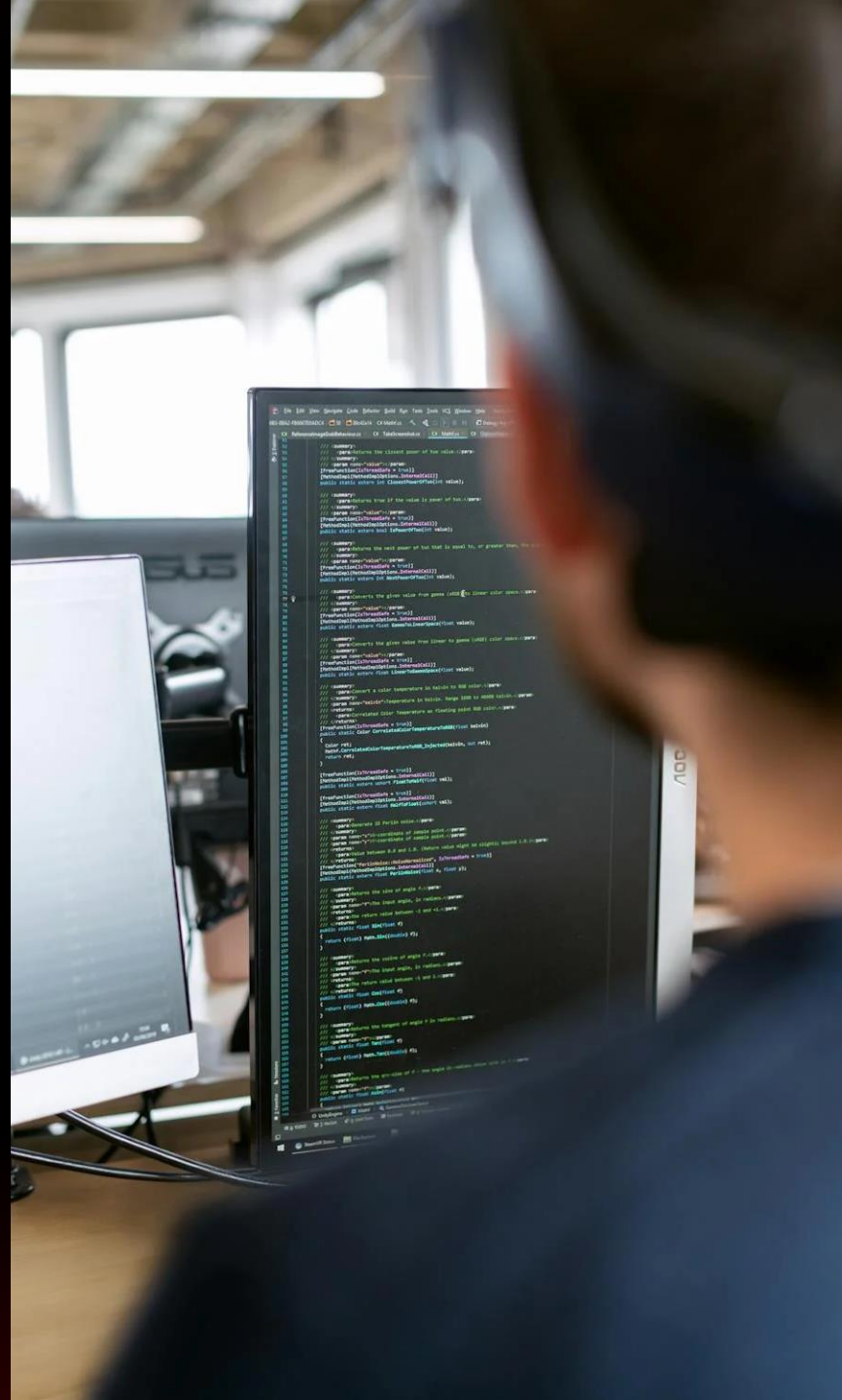


Генерация SBOM

- Вендор должен предоставлять подписанный SBOM на свое ПО, но мало кто это делает

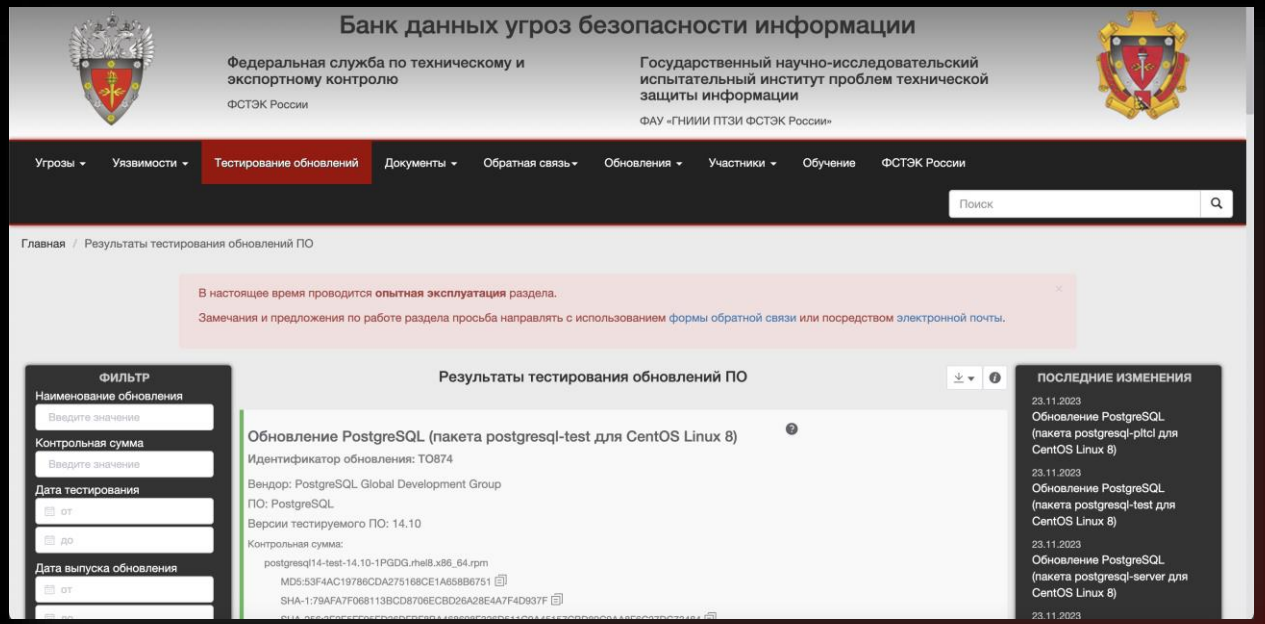
```
$ syft neo4j:latest
 ✔ Parsed image
 ✔ Cataloged packages      [376 packages]
NAME                              VERSION                          TYPE
CodePointIM                       11.0.15
java-archive
FastInfoset                       1.2.16
java-archive
...
util-linux                        2.36.1-8+deb11u1                 deb
wget                              1.21-1+deb11u1                   deb
zlib1g                            1:1.2.11.dfsg-2+deb11u1          deb
zstd-jni                          1.5.0-4
java-archive
zstd-proxy                        4.4.8
java-archive
```

Syft



Тестирование обновлений

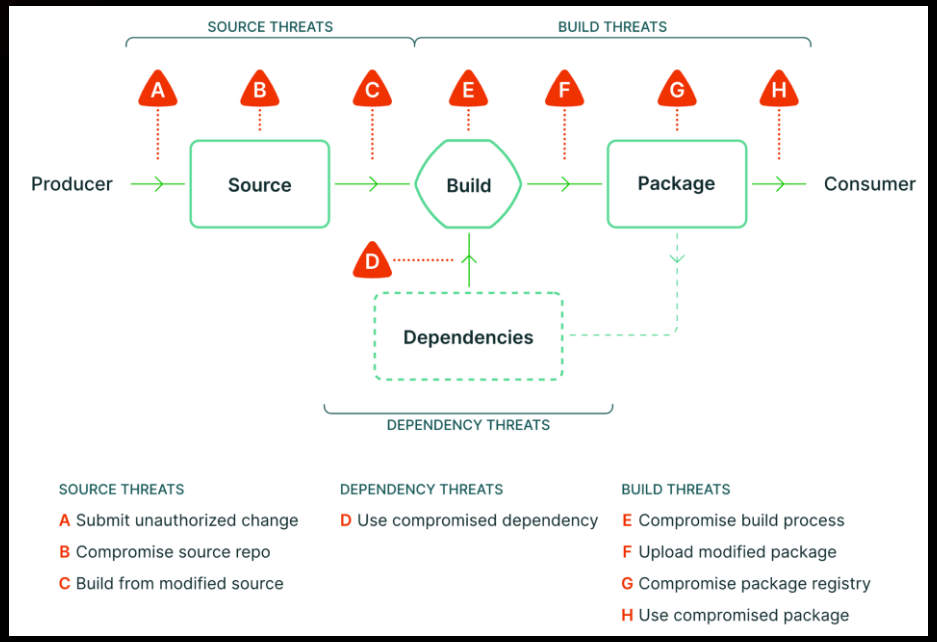
- Песочница
- Тестовый сегмент
- БДУ и методика ФСТЭК



https://bdu.fstec.ru/software-section/updates

SLSA

- Стандарт Supply-chain Levels for Software Artifacts для защиты ПО от угроз на цепочку поставок

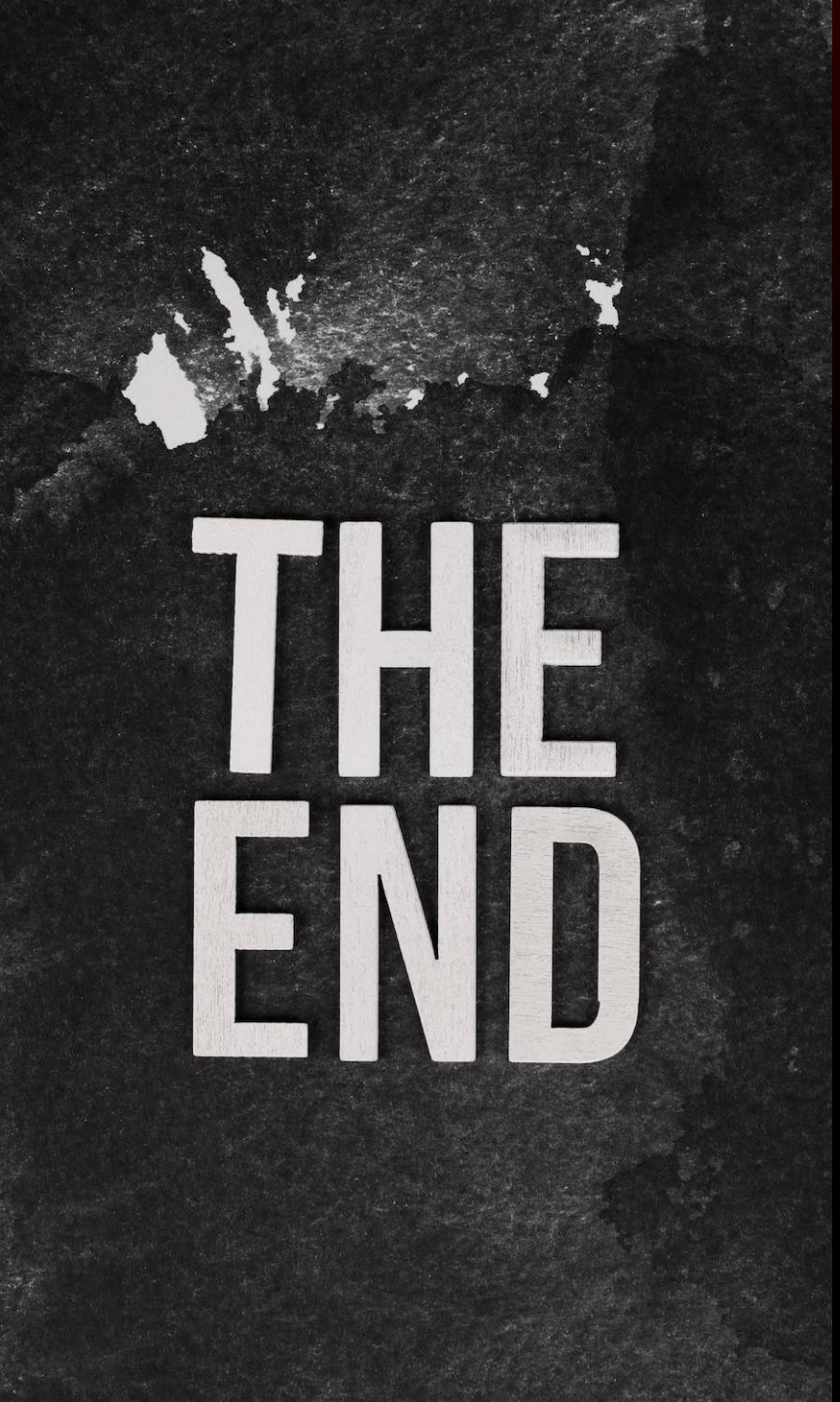


TLS fingerprinting

- Обнаружение аномалий по отпечатку клиентского ПО в сетевом трафике (TLS + хеши JA3/JA3S)
  - Выявление JA3 хэшей, характерных для популярных ПО и сетевых библиотек языков программирования
  - Выявление конкретного ВПО по хэшам JA3\JA3S
  - Выявления нового хэша JA3, ранее непоявляющегося в сети
  - Выявления хэшей JA3 не из белого списка
  - Выявления хэшей JA3\JA3S из черного списка
  - Выявление JA3 хэшей, не характерных для системы

Регистрация событий

- Как подрядчик обеспечивает сбор доказательств несанкционированной деятельности?
- Как долго подрядчик хранит логи? Возможно ли увеличение этого срока?
- Можно ли организовать хранение логов во внешнем хранилище? Как?



В качестве заключения

- Поймите, что типично и нетипично для подрядчиков разных типов
- Уменьшите площадь атаки за счет регулярного мониторинга защищенности
- Поставьте на мониторинг разные каналы взаимодействия с подрядчиками
- Мониторьте известные атаки и аномальное поведение

Спасибо

alukatsky@ptsecurity.com