Механизмы Kubernetes® против атак Supply Chain

Безопасность

Сергей Канибор

R&D / Container Security,
Luntry

Сергей Канибор

R&D / Container Security в Luntry

Специализируюсь на безопасности контейнеров и Kubernetes®

Багхантер

Редактор Telegram-канала k8s (in)security

Спикер: PHDays, OFFZONE, VK Kubernetes Conf, DevOops, HackConf, CyberCamp, БеКон и др.

Agenda

1. Supply Chain 101
2. От теории к практике
3. SolarWinds в Kubernetes®
4. Нет бэкдора лучше уязвимости

Supply Chain 101

CNCF Security Technical Advisory Group

Software Supply Chain

Supply chain compromises are a powerful attack vector. In cloud native deployments everything is software-defined, so there is increased risk when there are vulnerabilities in this area. If an attacker controls the supply chain, they can potentially reconfigure anything in an insecure way.

What are supply chain vulnerabilities and their implications?

The Catalog of Supply Chain Compromises provides real-world examples that help raise awareness and provide detailed information that let's us understand attack vectors and consider how to mitigate potential risk.

On mitigating vulnerabilities

There is on-going work to establish best practices in this area. The list of types of supply chain compromises in the catalog of supply chain compromises suggests some mitigation techniques for the more well understood categories.

Supply chain security paper

STAG (Security Technical Advisory Group) has put work into a comprehensive software supply chain paper highlighting best practices for high and medium risk environments. Please check out the paper and corollary secure supply chain assessment document to learn more.

For information about contributing to the document or providing feedback, please refer to the README.

github.com/cncf/tag-security/tree/main/supply-chain-security

CNCF SSCP

Software Supply Chain Best Practices

GITHUB.COM/CNCF/TAG-SECURITY

clck.ru/3BV529

CNCF Security Whitepaper

cncf.io/reports/cloud-native-security-whitepaper

Software Secure Factory Whitepaper

github.com/cncf/tag-security/blob/main/supply-chain-security/secure-software-factory/Secure_Software_Factory_Whitepaper.pdf

SLSA

Requirement		Required at SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source	Version Controlled		✓	✓	✓
	Verified History			✓	✓
	Retained Indefinitely			18 mo.	✓
	Two-Person Reviewed				✓
Build	Scripted	✓	✓	✓	✓
	Build Service		✓	✓	✓
	Ephemeral Environment			✓	✓
	Isolated			✓	✓
	Parameterless				✓
	Hermetic				✓
	Reproducible				◯

Requirement		Required at SLSA 1	SLSA 2	SLSA 3	SLSA 4
Provenance	Available	✓	✓	✓	✓
	Authenticated		✓	✓	✓
	Service Generated		✓	✓	✓
	Non-Falsifiable			✓	✓
	Dependencies Complete				✓
Common	Security				✓
	Access				✓
	Superusers				✓

◯ — required unless there is a justification

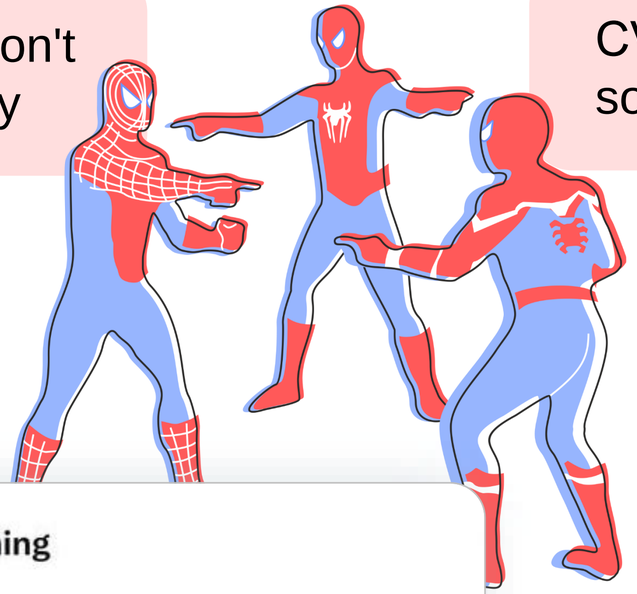
security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html

Безопасность Supply Chain = контроль SBOM?

SBOMs don't solve security

Signatures don't solve security

CVEs don’t solve security



SBOMs don't stop SolarWinds

signatures don't stop Log4j

SLSA doesn't stop typosquatting

I guess… we'll do nothing 🤡

«Человек-паук» © The Walt Disney Company, 1994–1998 гг.


KubeCon | CloudNativeCon

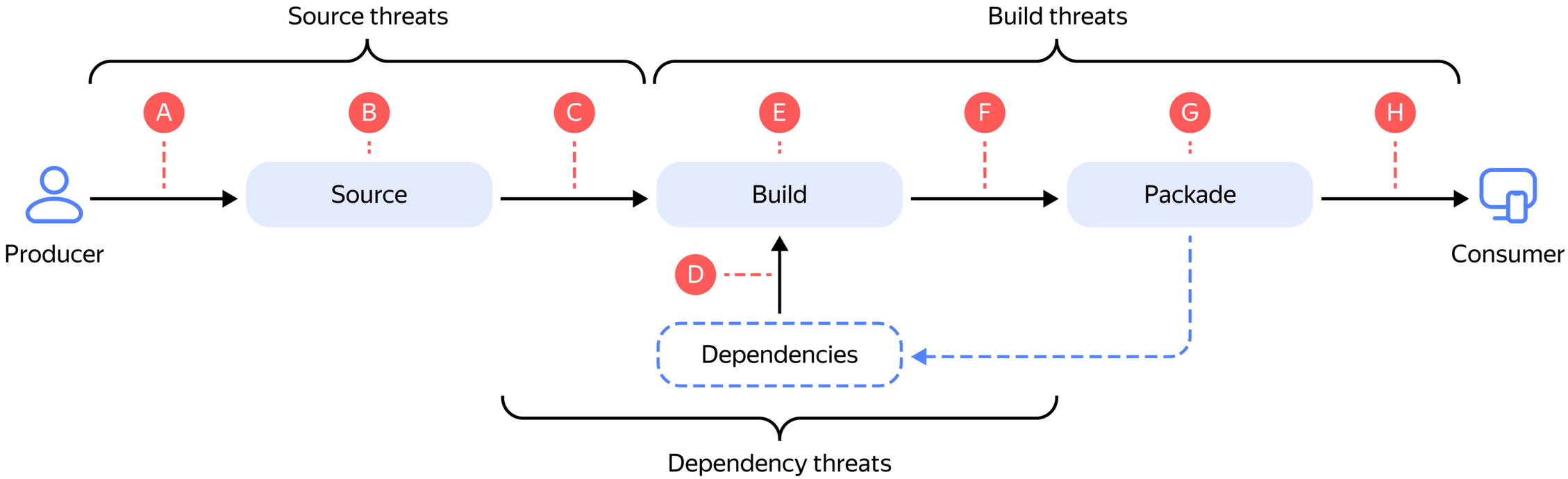
Europe 2023

Malicious Compliance: Reflections on Trusting Container Scanners

Ian Coldwater, Independent; Duffie Cooley, Isovalent; Brad Geesaman, Ghost Security; Rory McCune, Datadog

youtube.com/watch?v=9weGi0csBZM

Supply Chain



Source threats

A. Submit unauthorized change
B. Compromise source repo
C. Build from modified source

Dependency threats

D. Use compromised dependency

Build threats

E. Compromise build process
F. Upload modified package
G. Compromise package repo
H. Use compromised package

От теории к практике

Build from modified resources — CVE-2019-15231

Атакующий модифицировал инфраструктуру сборки, добавив дополнительный скрипт для возможности получения RCE

Build from modified resources — CVE-2019-15231

~~Атакующий модифицировал инфраструктуру сборки, добавив дополнительный скрипт для возможности получения RCE~~

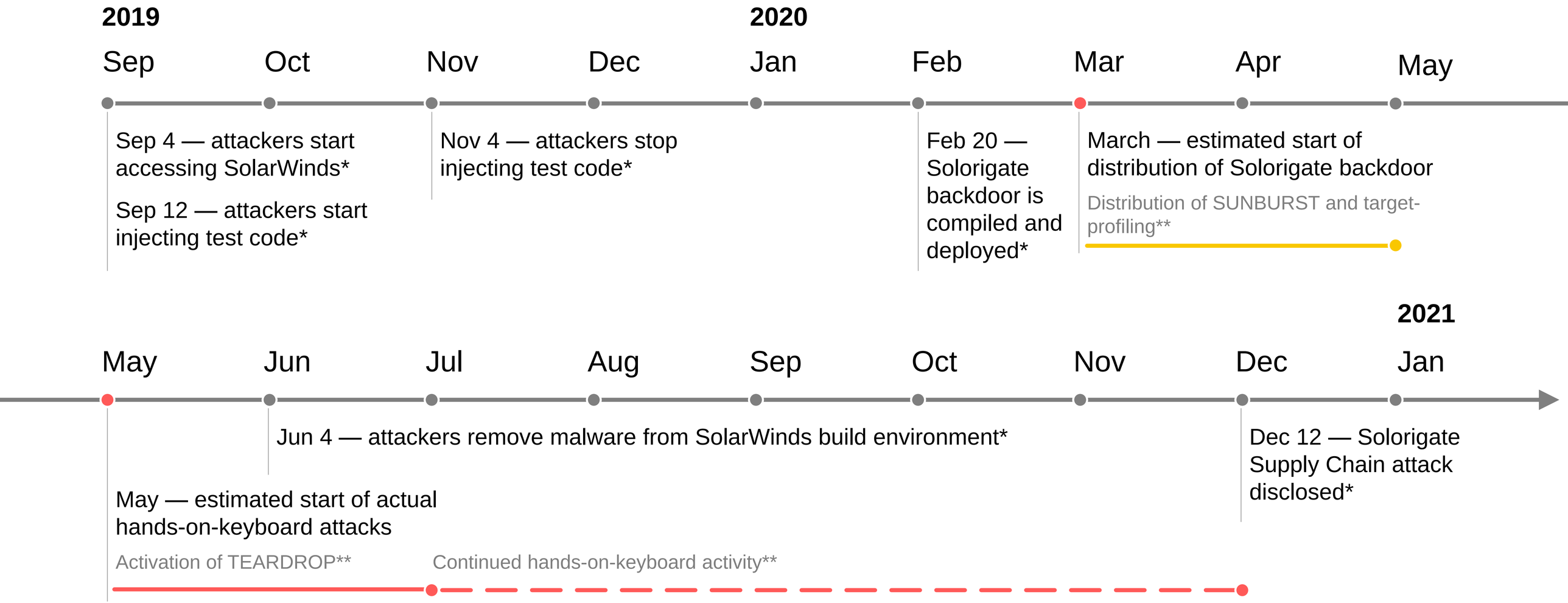
AppArmor

Network Policy

SecurityContext

SolarWinds в Kubernetes®

Supply Chain Attack SolarWinds



* Info disclosed by SolarWinds.
** Estimated timeline of activity based on forensic analysis.

SolarWinds в Kubernetes

Алгоритм действий бэкдора

- Выжидание 12–14 дней перед первичным соединением с C2
- Сбор информации о сервере (username, IP, OS)
- Соединение с C2
- Загрузка дополнительного компонента для развития атаки

Алгоритм действий бэкдора

- Выжидание 12–14 дней перед первичным соединением с C2
- ~~Сбор информации о сервере (username, IP, OS)~~ AppArmor
- Соединение с C2
- Загрузка дополнительного компонента для развития атаки

Алгоритм действий бэкдора

- Выжидание 12–14 дней перед первичным соединением с C2
- ~~Сбор информации о сервере (username, IP, OS)~~ AppArmor
- ~~Соединение с C2~~ Network Policy
- Загрузка дополнительного компонента для развития атаки

Алгоритм действий бэкдора

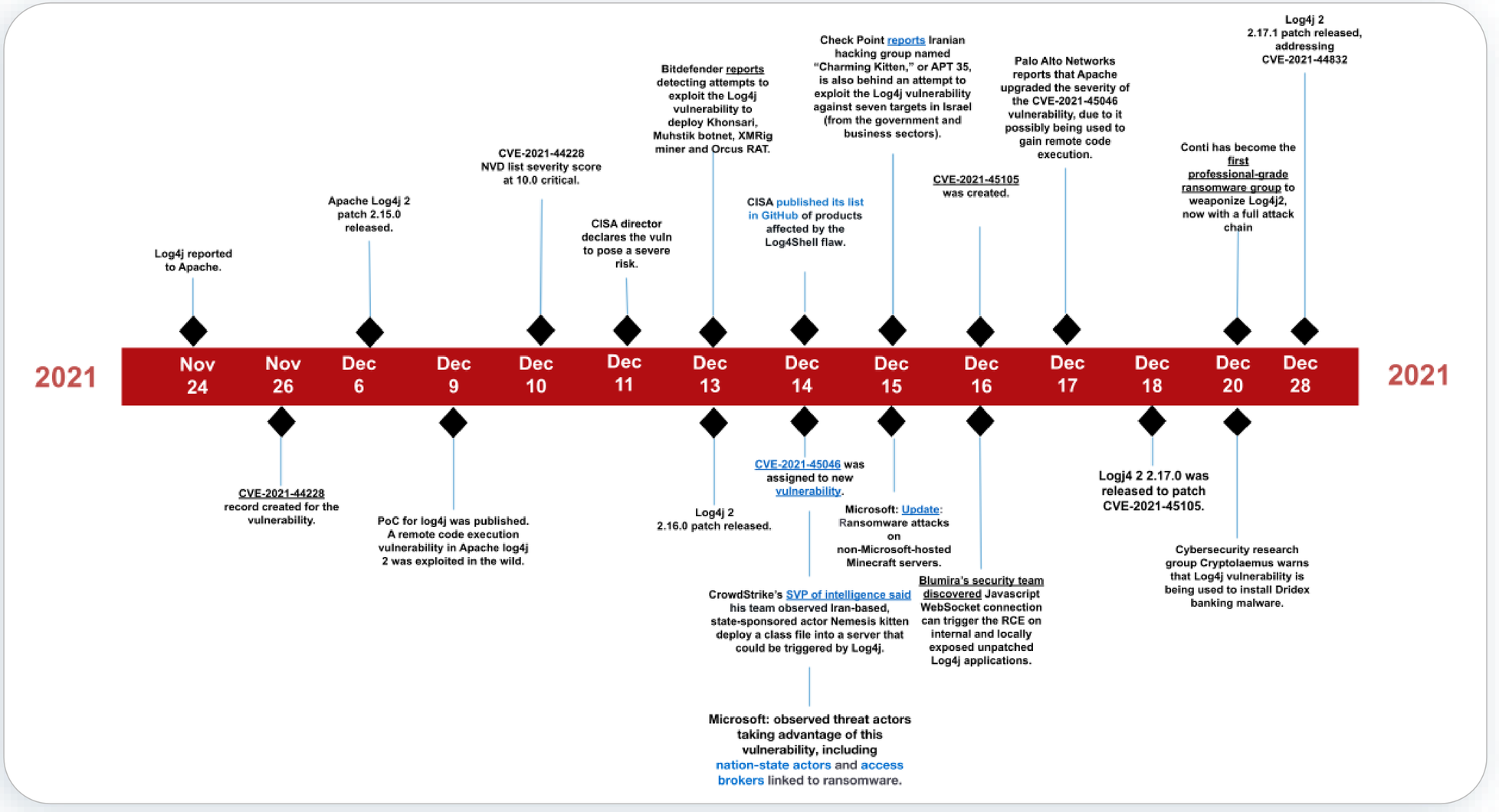
- Выжидание 12–14 дней перед первичным соединением с C2
- ~~Сбор информации о сервере (username, IP, OS)~~ AppArmor
- ~~Соединение с C2~~ Network Policy
- ~~Загрузка дополнительного компонента для развития атаки~~ Network Policy

Закладка

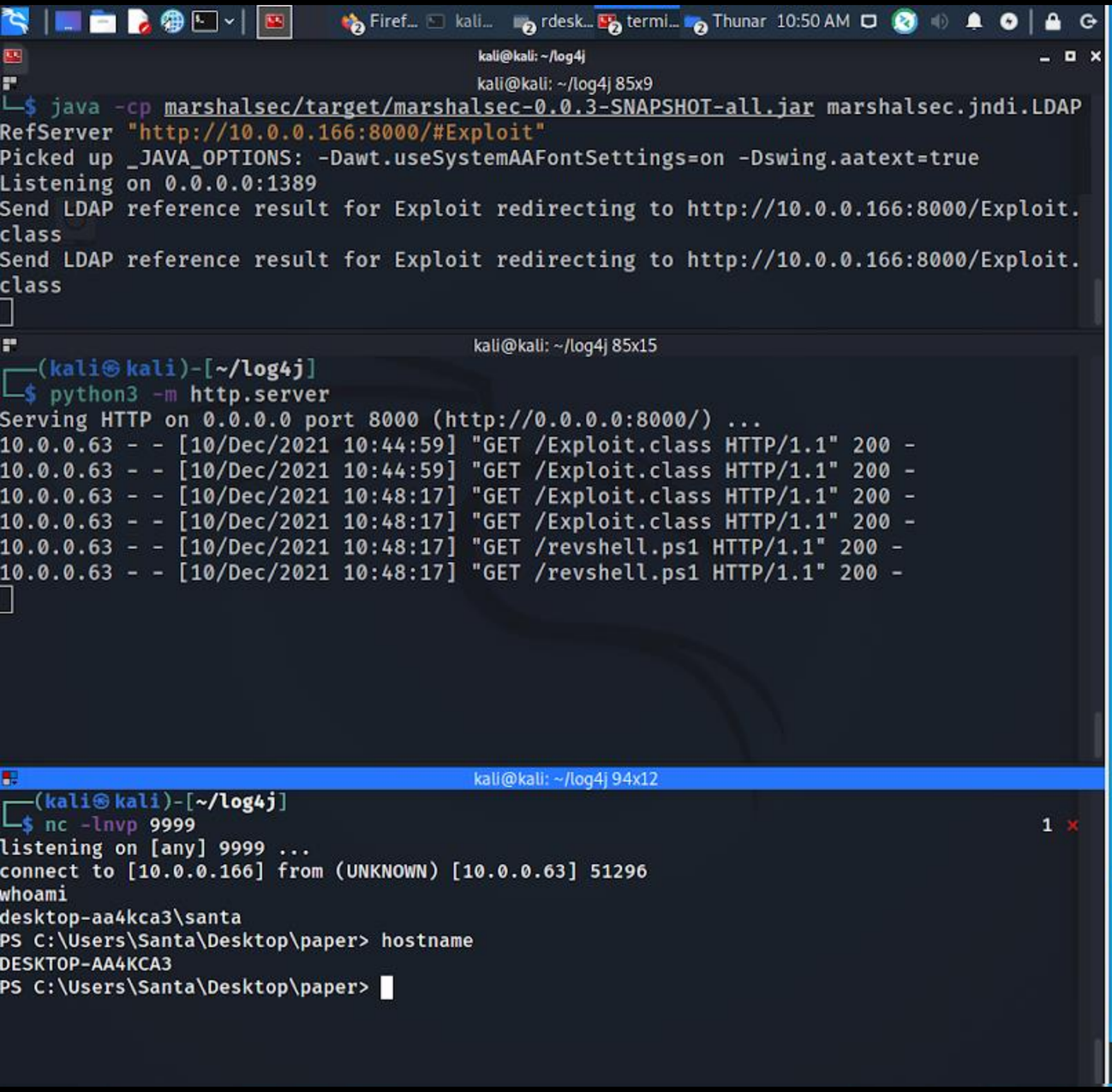
Уязвимость

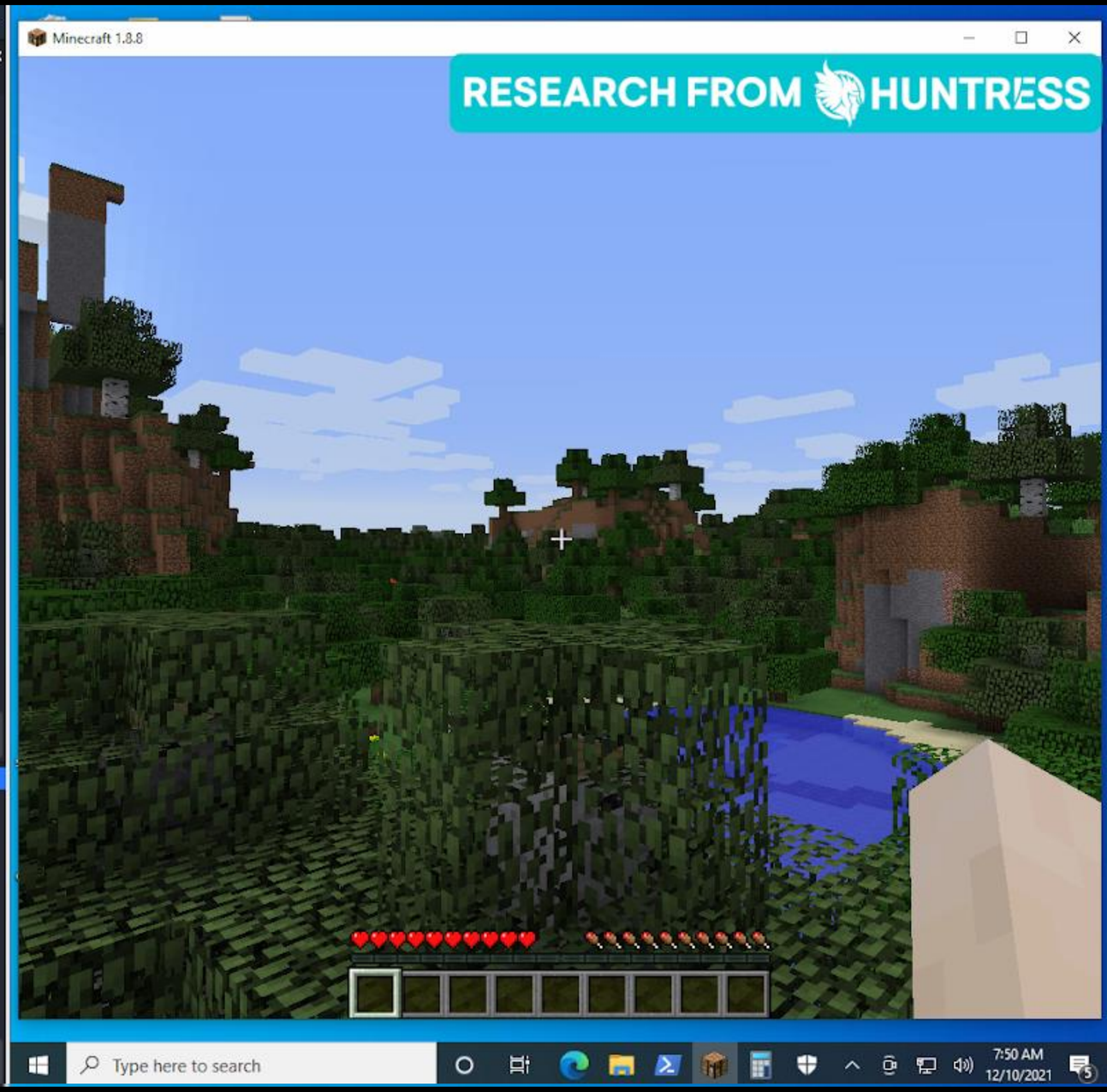
Нет бэкдора лучше уязвимости

CVE-2021-44228 aka Log4shell



dokumen.pub/software-transparency-supply-chain-security-in-an-era-of-a-software-driven-society-2022951423.html





jeffreykopcak.com/tag/soundcard/

Log4shell

- Уязвимость Log4j активируется полезной нагрузкой, где сервер делает запрос к some-attacker.com через Java Naming and Directory Interface (JNDI)
- Ответ инжектится в процесс
- RCE

Log4shell

- ~~Уязвимость Log4j активируется полезной нагрузкой, где сервер делает запрос к some-attacker.com через Java Naming and Directory Interface (JNDI)~~ Network Policy
- ~~Ответ инжектится в процесс~~
- ~~RCE~~
- Всё!

Выводы

Supply Chain могут появиться
в любой момент и в любом
компоненте

Можно защищаться
как от известных,
так и от неизвестных угроз

Стройте безопасность
из того, что всё взломано

Механизмы Kubernetes®
позволяют делать это гибко
и декларативно

Спасибо за внимание!

Безопасность

t.me/k8security

Задавайте вопросы в чате:
t.me/kuberconf/11726

Сергей Канибор

R&D / Container Security,
Luntry