Supply Chain Threats

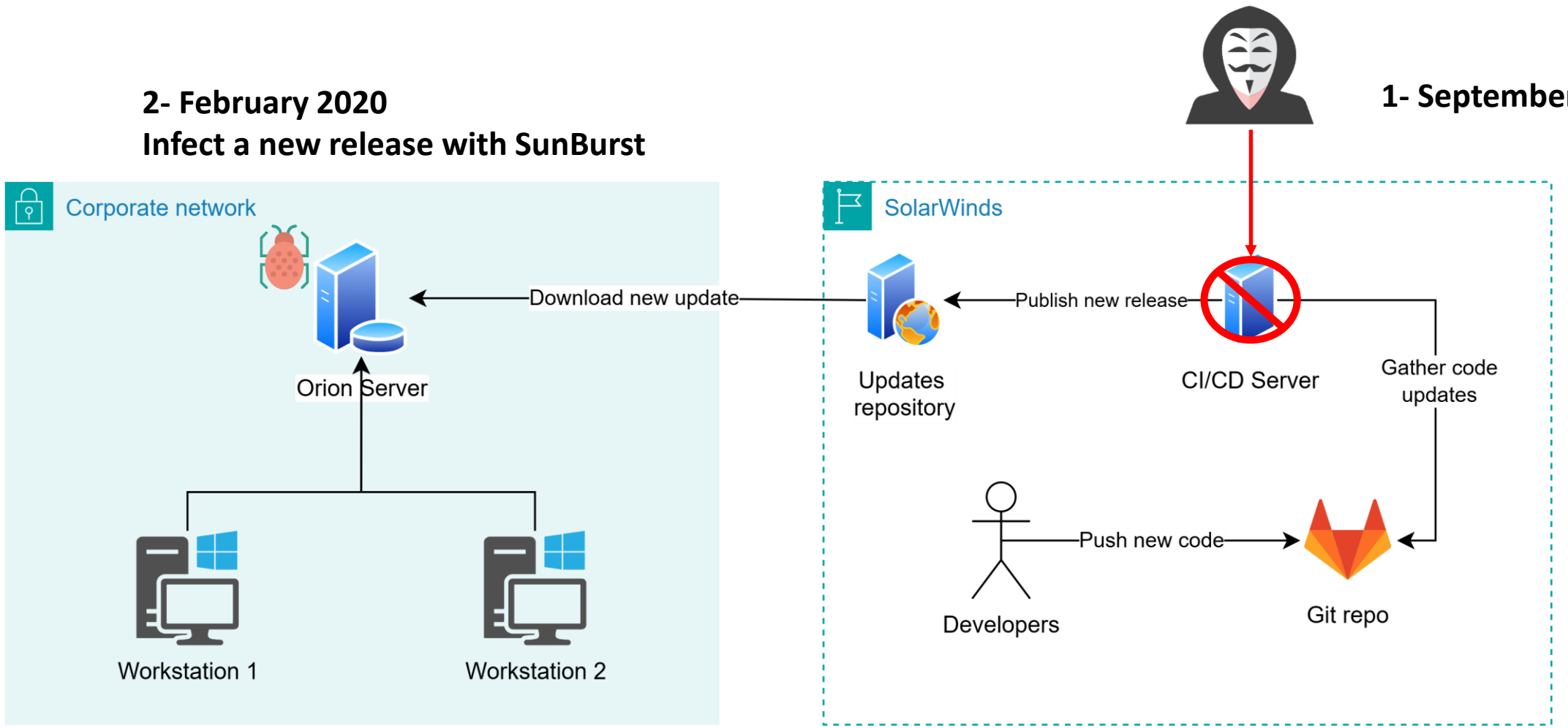
Storytime

- **It's 2020** – You are the CTO of **ITHeaven**
- The Company:
  - Provide Web Services hosting to Third Parties
  - More than 50 VMs running in parallel
- **Observability** is a challenge given the amount of devices to monitor
- No resources available to build an observability stack from scratch
  - **Decision**: Use an existing on-premise solution
    - Solarwinds Orion

Solarwinds Orion

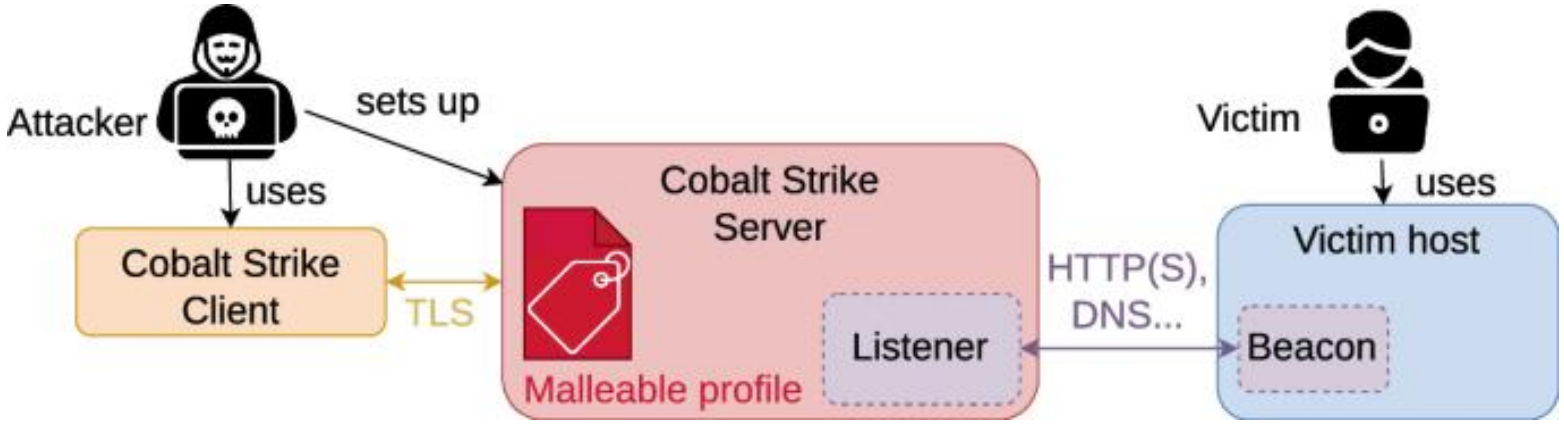
- Enterprise-class infrastructure management software
  - Manage and monitor data centers and IT infrastructure
- Features
  - Centralized management of physical and virtual infrastructure
  - Real-time monitoring (Dashboards)
  - Alerting
  - Reporting
- Requires to install an on-premise platform server within the company network
  - + Need to install an agent on the assets to monitor

Solarwinds Orion



Solarwinds Orion - SunBurst

- Command-an-Control (C2) Attack Schema
  - Cobalt Strike beacon
- Provide remote access to attackers
  - Privilege escalation
  - Spyware
  - Ransomware
  - DDoS

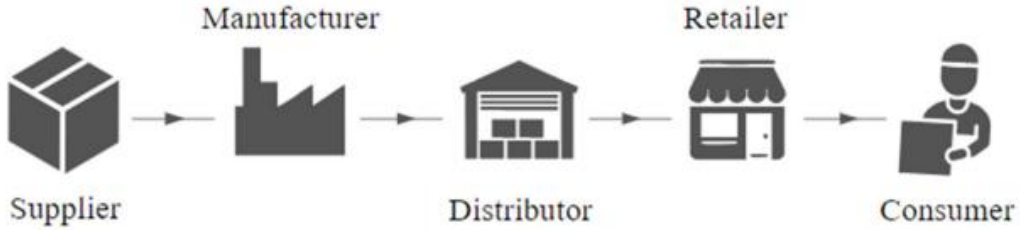


Solarwinds Orion

- Fire-Eye detects an intrusion in their systems via Orion platform (November 2020)
  - **8 months** since the malicious update release
- More than 18.000 customers installed the malicious update
  - Public sector and private companies affected
- **Software Supply Chain Attack**

Supply Chain

- **Traditional Supply Chain**
  - Turning raw materials into finished goods and products
- **Digital Supply Chain**
  - Assembling components into a funcional service or experience
  - *Trust is a requirement*



+ Actors
+ Components
+ Dependencies

Risk

The Four Pillars of the Digital Supply Chain

- **Software**
  - Open source libraries (GitHub)
  - Software-as-a-Service (SaaS)
  - Commercial Software
    - Microsoft 365 / Google Workspace
- **Hardware**
  - Network equipment
    - Routers / Firewalls / Switches
  - Workstations / Bare-Metal Servers
- **Services**
  - Cloud Providers (AWS / GCP / Azure)
  - Marketing agencies
- **People**
  - Freelancers
  - Consultants

Vendor Lock-In

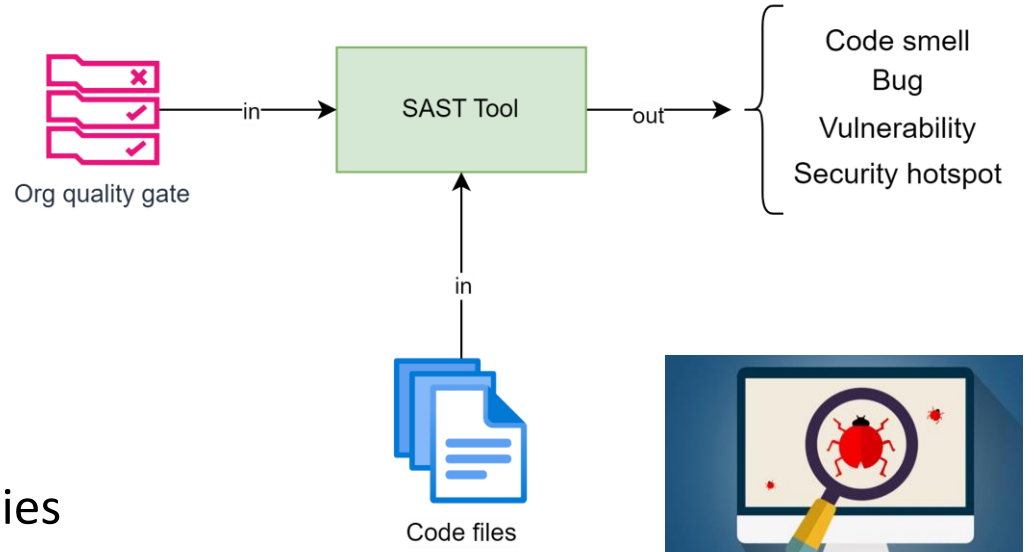
Security Threats

Attack Vector: Software

- SolarWinds Orion lessons:
  - **A supplier's risk is your risk**
    - The security of your third-party software directly impacts your own security and reputation
  - **No vendor is too big to fail**
    - Even large and renowned software companies can be compromised
      - Infrastructure and misconfigurations flaws
      - **Software vulnerabilities**
  - Software vendors must embrace a **Quality-First policy**
    - **Shift-Left Paradigm**

Quality-First: Software - SAST

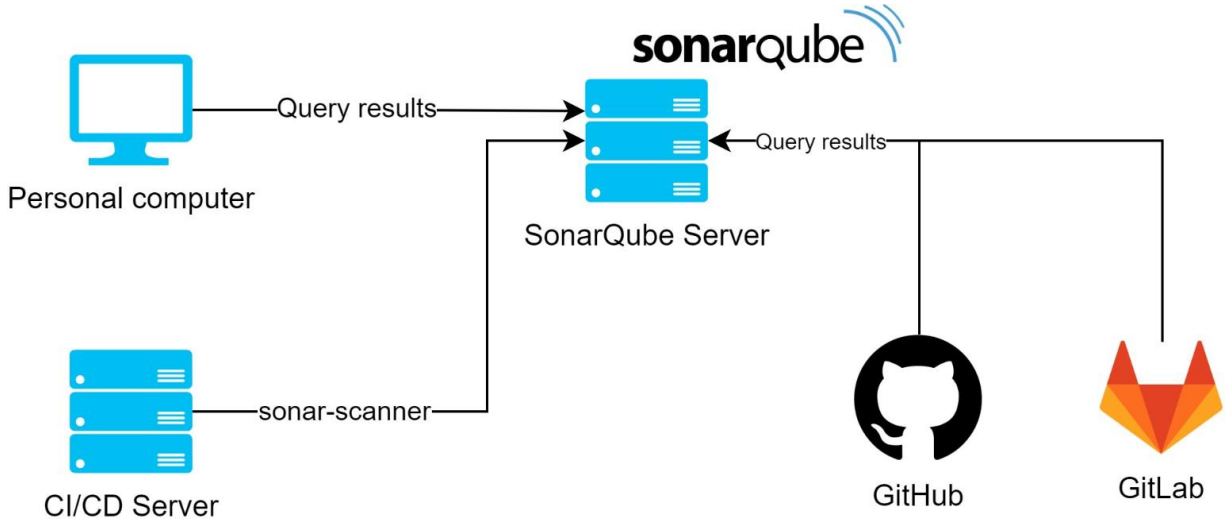
- How do software companies enforce quality checks before release?
- **Static Application Secure Testing (SAST)**
  - Source code analysis before compilation
  - **White Box Testing**
  - Scans for insecure patterns
  - Duplicated Code (Technical Debt)
  - Code Coverage
  - Verifies compliance with security and quality policies
  - Enforces organizational security related requirements



sonarqube

Quality-First: Software - SAST

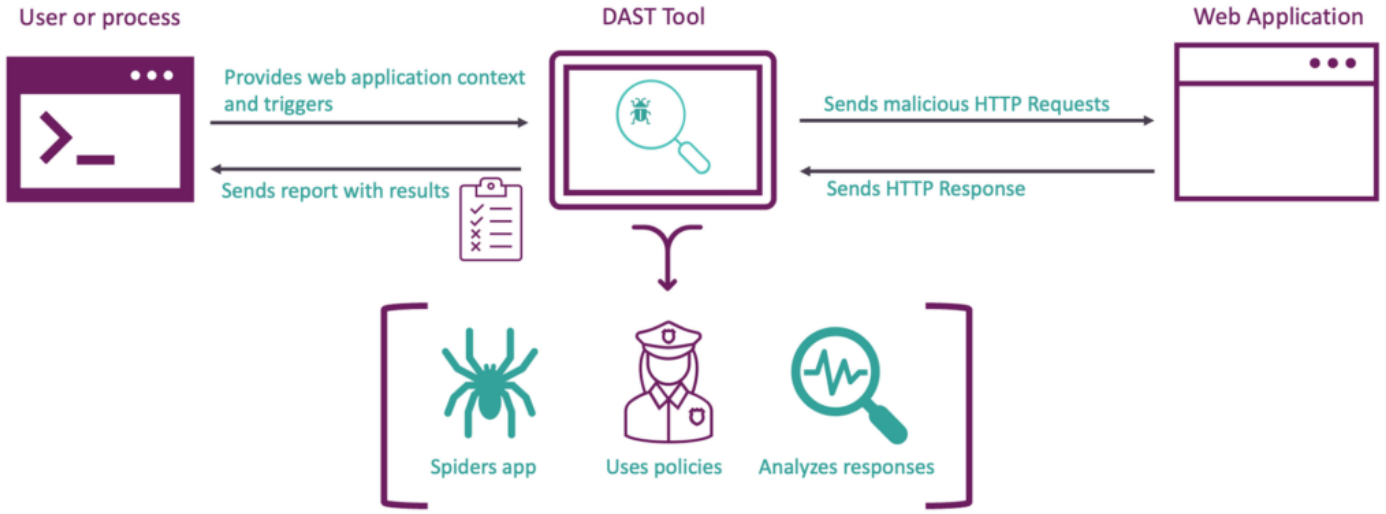
- **SonarQube**
  - **Features**
    - Static code analysis
    - Quality metrics
    - Helps to identify and manage technical debt
  - Easy integration with CI/CD tools
  - User-friendly graphical interface



sonarqube

Quality-First: Software - DAST

- Dynamic Application Security Testing (DAST)
  - Runtime analysis (or analysis during execution)
  - Simulates malicious requests
  - **Black Box Testing**
  - Detects vulnerabilities related to the service runtime environment



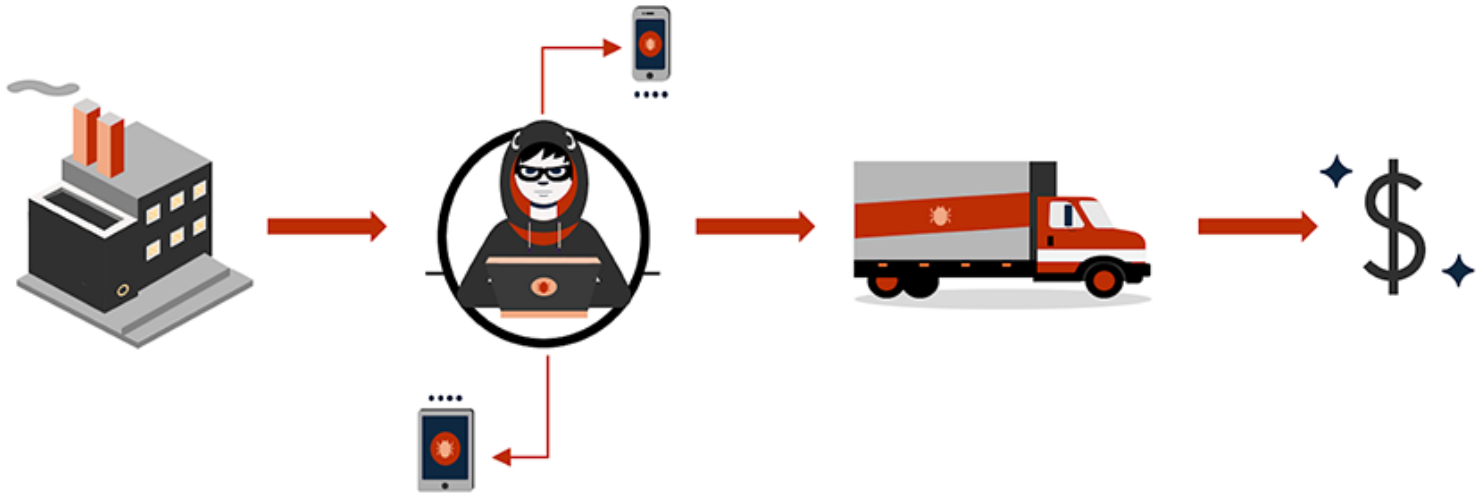
Quality-First: Software - DAST

- OWASP ZAP
  - Open Worldwide Application Security Project
  - Open Source
  - ZAP (Zed Attack Proxy)
  - Includes an automated web-application scanner
  - Compatible with APIs
  - Build uppon OWASP Top Ten

OWASP
Zed Attack Proxy

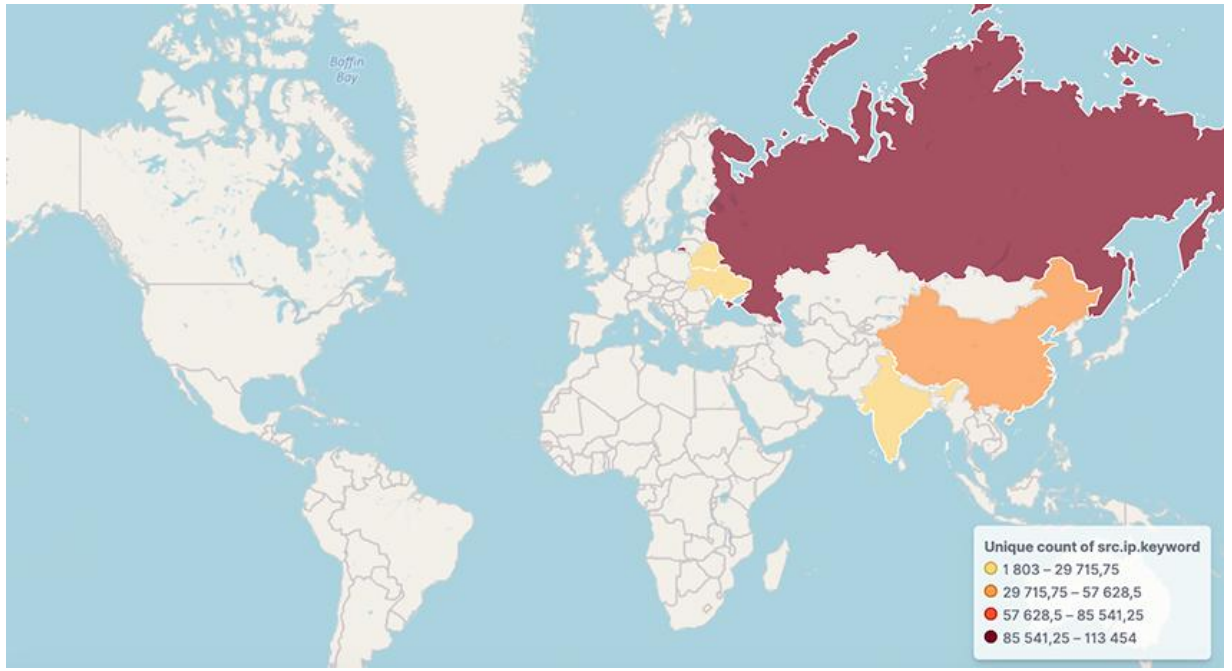
Attack Vector: Hardware Compromise

- **BadBox (2023)**
  - Cybercriminal operation
  - Selling off-brand Android TV Boxes and Smartphones with preinstalled malware at firmware level
  - The device is infected before it reaches the final consumer



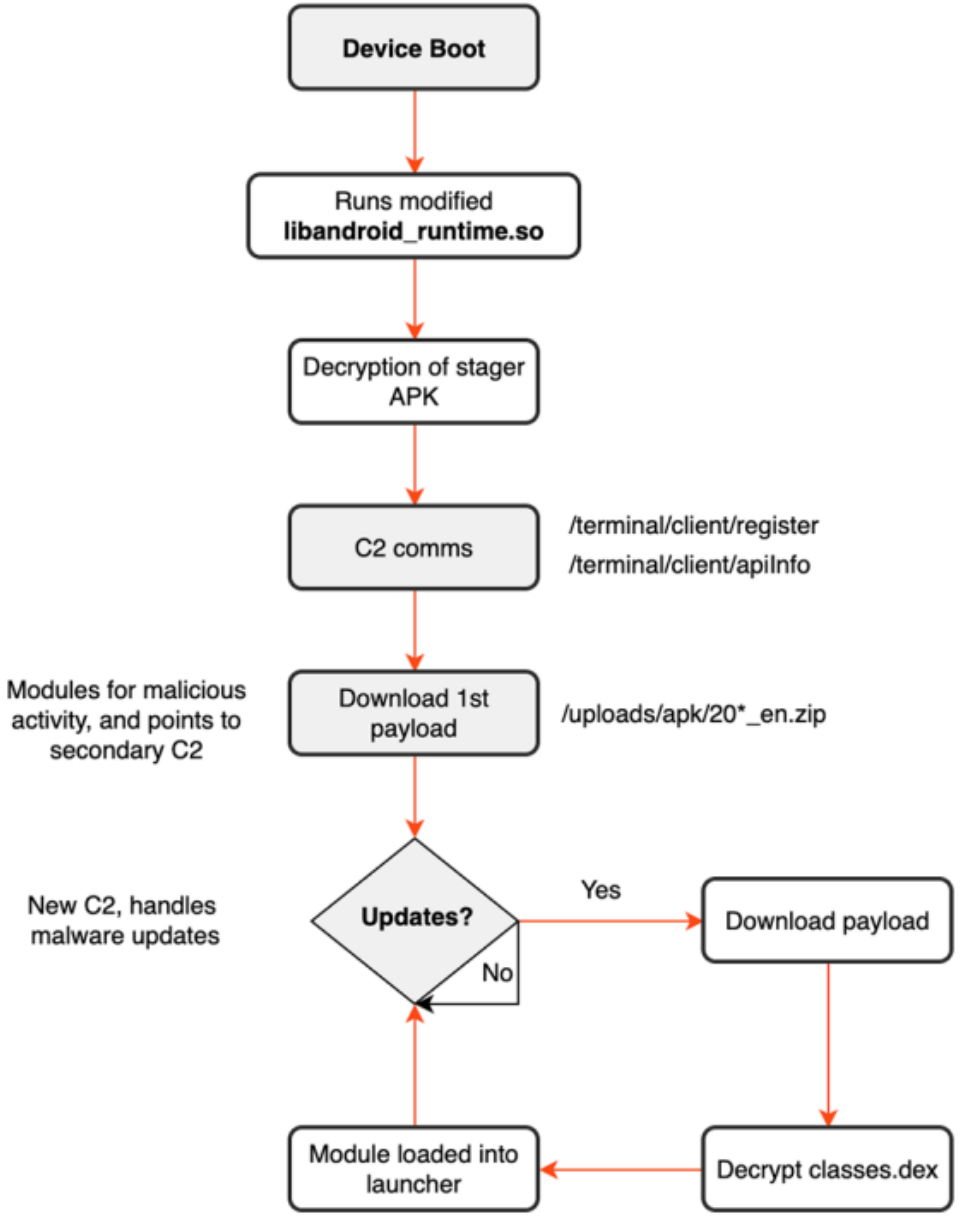
Attack Vector: BadBox

- Estimated peak of **192.000 BadBox infected devices**
  - Top affected countries: Russia, China, India, Belarus, Brazil and Ukraine



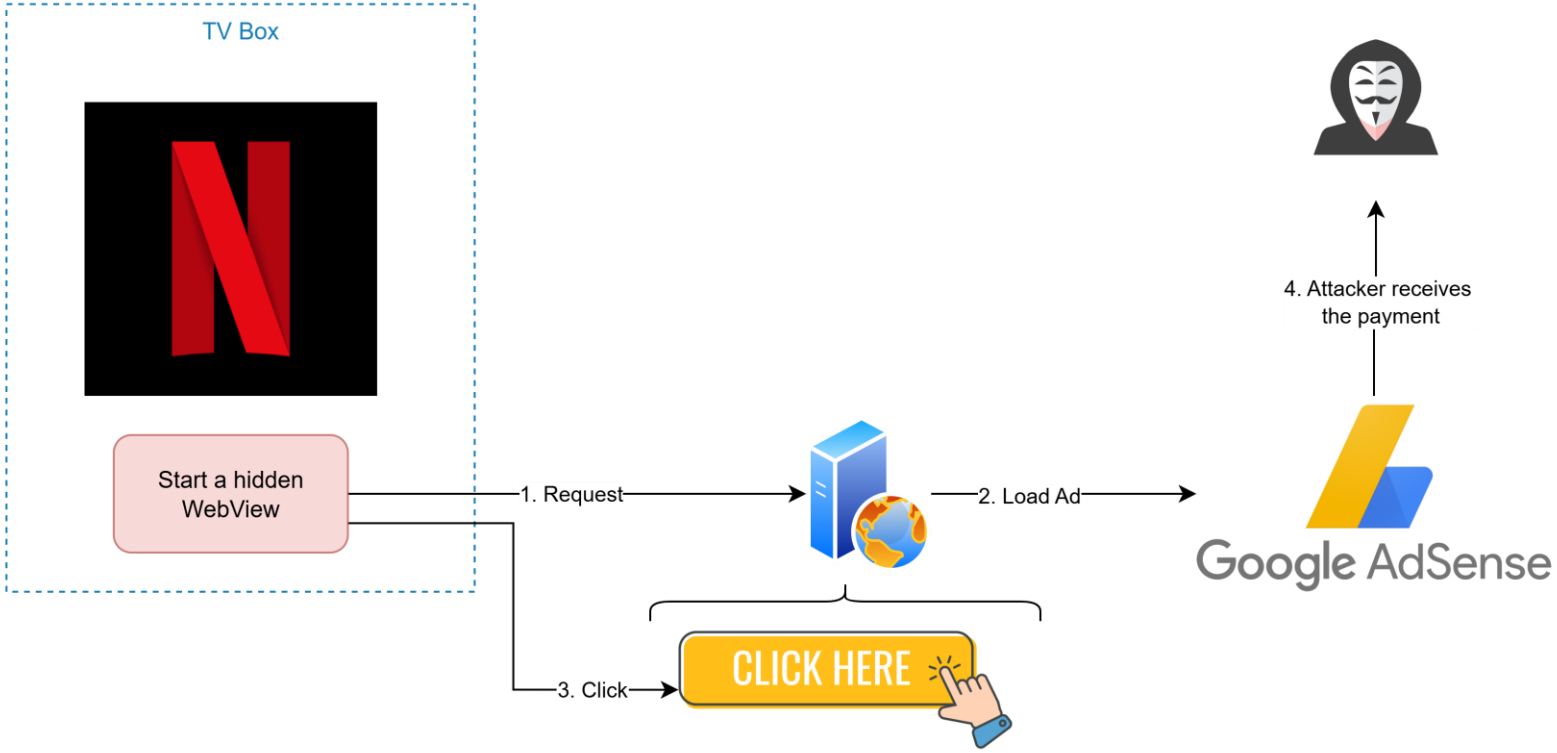
Attack Vector: BadBox

- Infection at ROM Level
  - Boot level libraries
- Use of a Stager encrypted script
- Auto-Update via C2 server
- Execution of the payload in the launcher



Attack Vector: BadBox

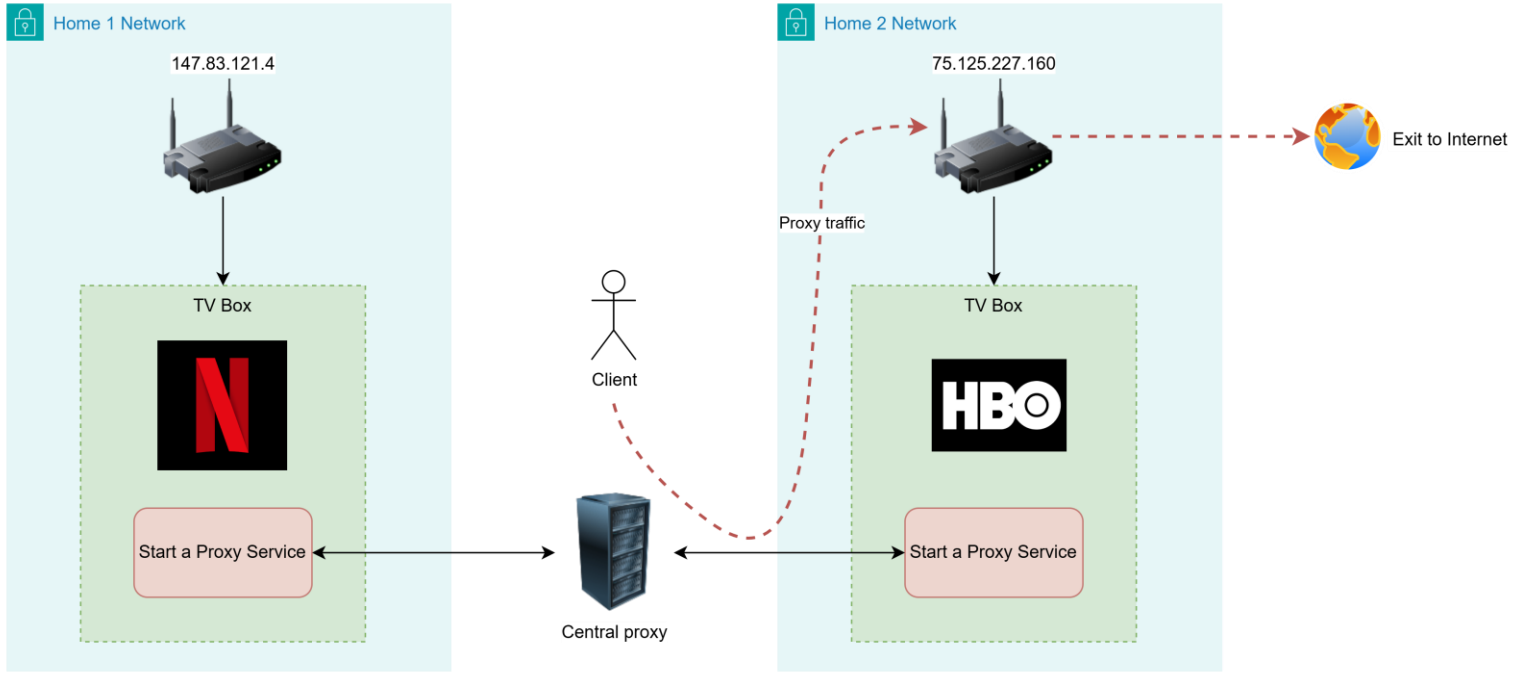
- Ad-Fraud Campaigns (PEACHPIT)
  - Load of webpages with ads via WebView



Attack Vector: BadBox

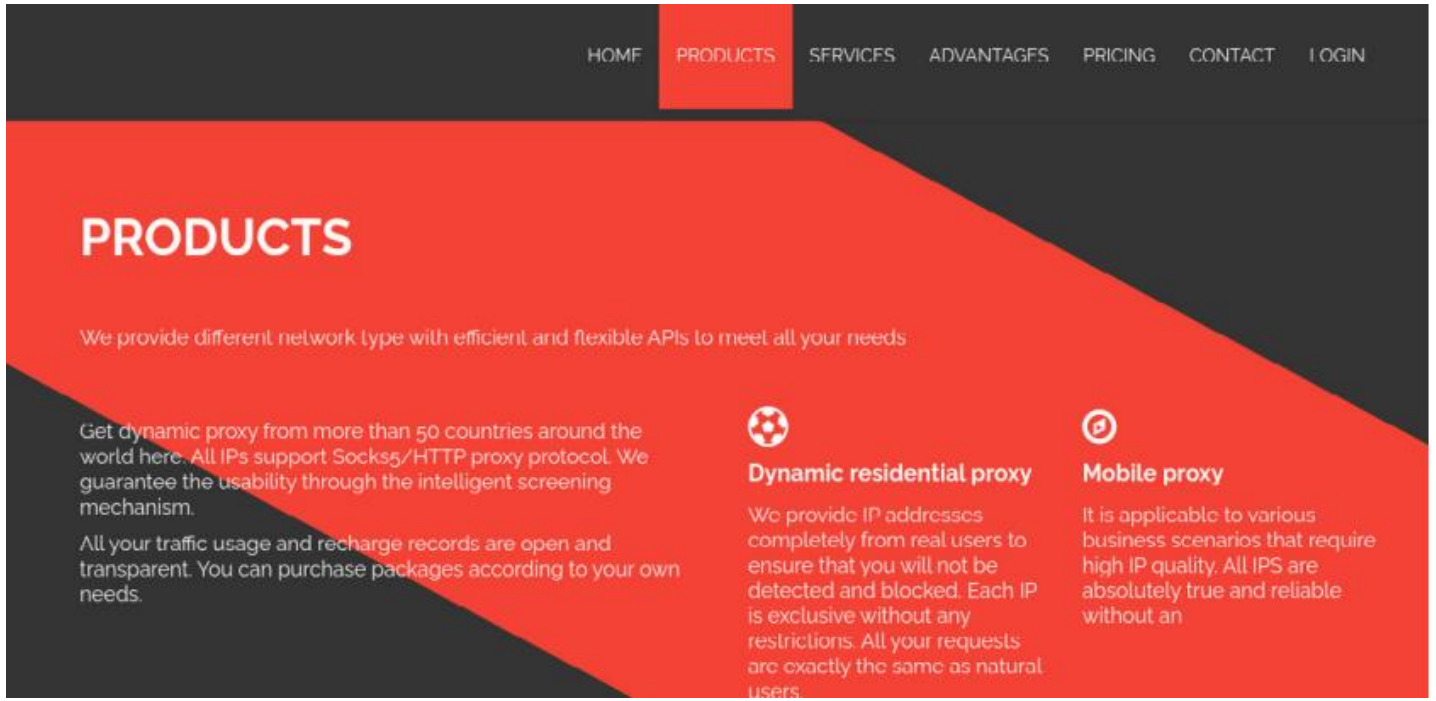
- Residential Proxy
  - Enroll the device into a residential proxy-network
  - Attackers get a revenue from users and Residential VPN providers
  - Users will exit to internet with your public IP as source

Help attackers to easily hide their tracks



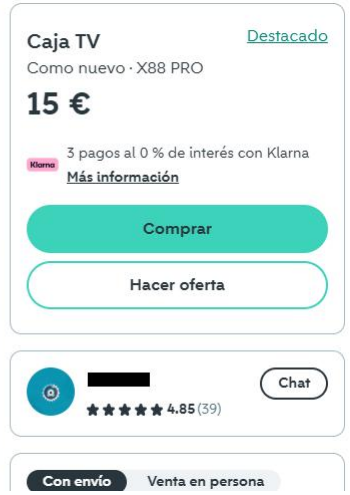
Attack Vector: BadBox

- Residential Proxy
  - Threat actors behind BadBox made this residential proxy service commercially available to interested customers



Attack Vector: BadBox

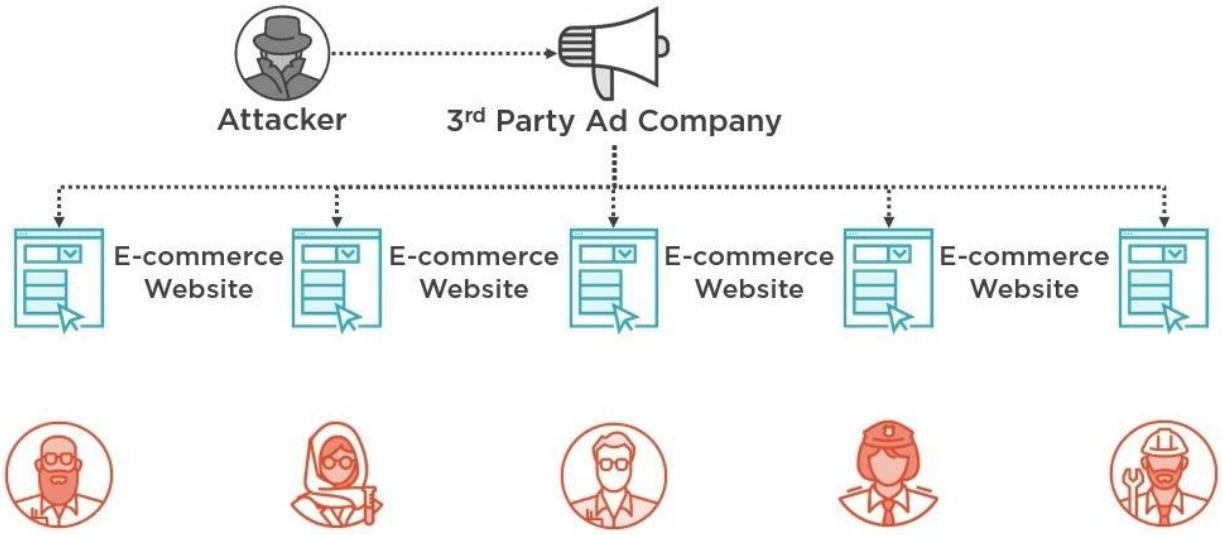
- Many of C2s associated to BadBox have been taken down
- Remainder devices should be considered *dormant*
  - The BadBox campaign can be **relaunched via OTA** at any time
- Infected devices are still available on the wild



https://github.com/DesktopECHO/T95-H616-Malware

Attack Vector: Third-Party Compromise

- Island hopping
  - Attackers target vulnerable third party vendors
  - Turn trusted business relationships into pathways for intrusions



Attackers target the weakest link in the supply chain

Attack Vector: Third-Party Compromise

- Examples [Spain]:
  - Mango (October 2025)
    - **Origin**: External marketing service
    - **Data**: Personal data for marketing (telf, e-mail)
  - Cruz Roja (October 2025)
    - **Origin**: External Contact Center
    - **Data**: Personal data of donors and partners
  - Iberdrola (May 2024)
    - **Origin**: Unknown third party party provider
    - **Data:** Personal Data (name, surname, DNI)

International: **SolarWinds Attack**

CIBERSEGURIDAD >

Mango sufre un ciberataque con acceso a nombres o teléfonos de clientes

La compañía textil asegura que no se ha visto comprometida información de carácter bancario. El origen está en un servicio externo de marketing

02 D'OCTUBRE Incidente de ciberseguridad en un proveedor de contact center

Cruz Roja Española informa de que un proveedor externo de la organización ha sufrido un ciberataque. Según los datos disponibles, podría ser que la información personal de personas socias y donantes, como datos bancarios y de afiliación, haya sido comprometida.

Queremos destacar que este incidente **no ha comprometido en ningún momento los sistemas internos de Cruz Roja Española, sino únicamente los del proveedor afectado.**

Un ciberataque a Iberdrola deja al descubierto los datos de 850.000 clientes en España

La energética niega que se hayan comprometido datos financieros, pero sí nombre, apellidos y número de DNI. Afirma haber avisado a todos los afectados

Defense - TPRM

- Zero Trust – Never Trust, always verify
  - Don’t trust anything nor anyone by default
- Define a Third-Party Risk Management (TPRM) policy

Defense - Certifications

- Formal audits verifying that a company has a structured cybersecurity program in place
  - Require security certifications before beginning a commercial engagement
- Examples
  - **ISO 27001**
    - Published by the International Organization for Standardization (ISO)
    - Defines security controls in IT Operations or data security
  - **Esquema Nacional de Seguridad (ENS)**
    - Real Decreto 311/2022
    - Includes required security measures at different levels:
      - Organizational, Operational and Protective measures
    - Required for the Spanish public sector and their providers
      - 3 level categories: Basic, Medium and High

Esquema Nacional de Seguridad

Defense - Certifications

- **PROS**:
  - Establishes a security baseline
  - Provides a common, recognized framework to assess the security level of a company
  - Demonstrates the company is proactive towards security
- **CONS**:
  - **Point-In-Time Snapshot**: A certificate proves a company was compliant on the day of the audit, not necessarily today
  - **Risk of "Paper Compliance"**: A certification doesn't guarantee a strong day-to-day security culture
  - **Doesn't cover everything**: Certifications are mean to suit all use-cases, might not cover specific services or products
- **Our strategy**:
  - Use certifications as a mandatory first step to establish a relation, but not the only step
  - Define your own questionnaires and contractual requirements to mitigate the potential security risks arising from he commercial relationships

References

- https://www.humansecurity.com/wp-content/themes/human/hubspot/hubfs/HUMAN_Report_BADBOX-and-PEACHPIT.pdf
- https://www.bitsight.com/blog/badbox-botnet-back
- https://cybersierra.co/blog/third-party-risk-management-guide/
- https://www.bitsight.com/learn/tprm/zero-trust