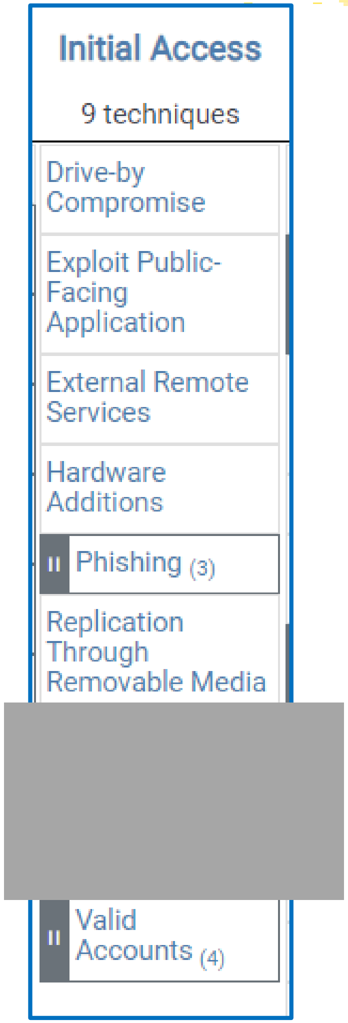
Initial Access: Advanced Techniques

Initial Access (I)



Initial Access

9 techniques

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (3)

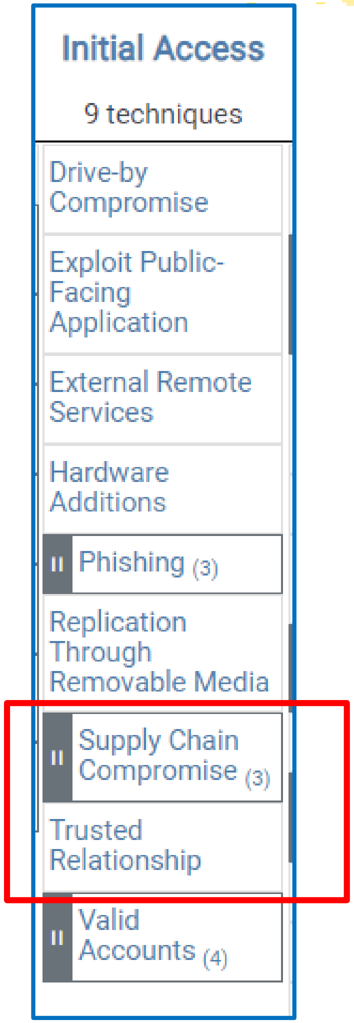
Replication Through Removable Media

[redacted]

Valid Accounts (4)

Nothing really surprising

Initial Access (II)



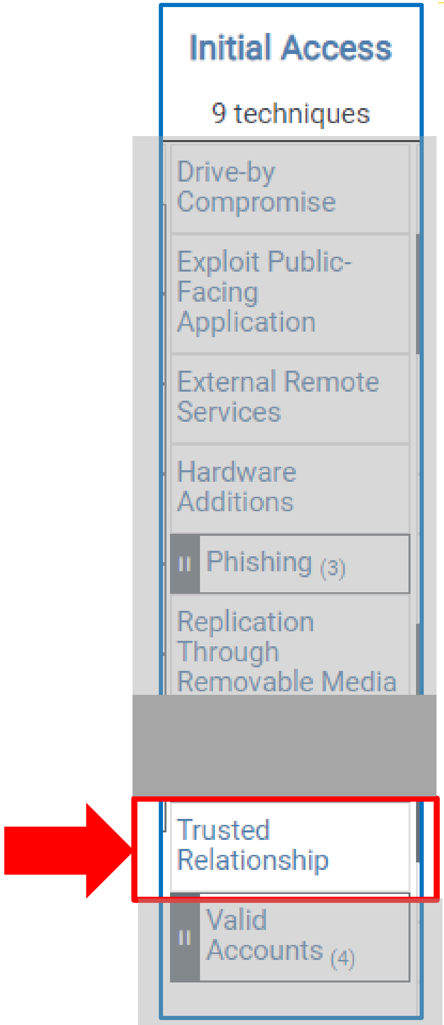
Initial Access

9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

BIG (REALLY BIG) HEADACHES

Trusted Relationship (I)



Initial Access

9 techniques

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (3)

Replication Through Removable Media

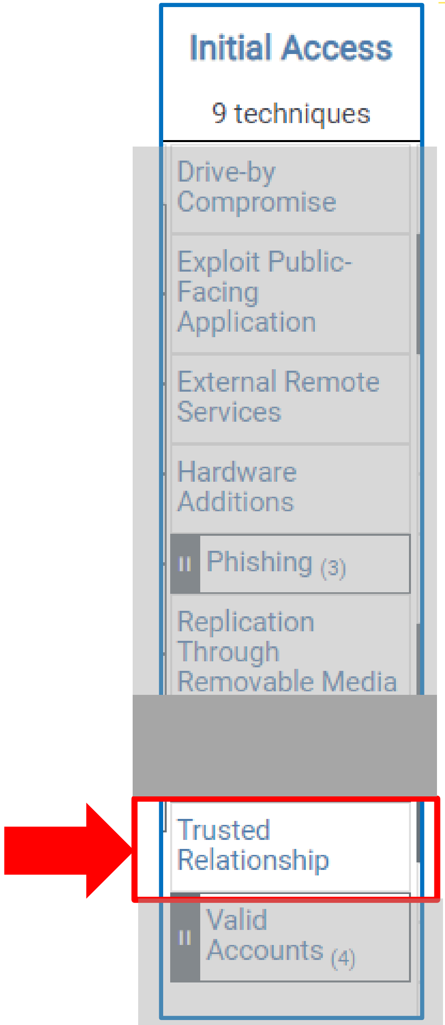
Trusted Relationship

Valid Accounts (4)

Organizations often grant **elevated access** to second or third-party **external providers** in order to allow them to **manage internal systems** as well as cloud-based environments.

Adversaries may **breach providers who have access to intended victims**. Access through trusted third party relationship abuses an existing connection that **may not be protected** or **receives less scrutiny** than standard mechanisms of gaining access to a network.

Trusted Relationship (II)



Initial Access

9 techniques

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (3)

Replication Through Removable Media

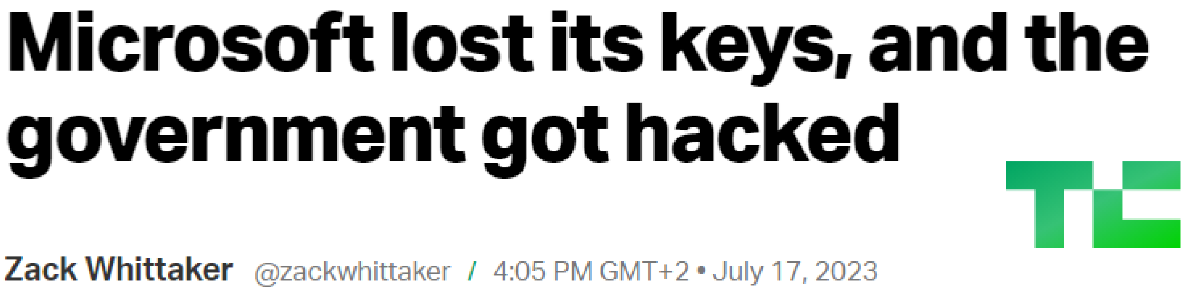
Trusted Relationship

Valid Accounts (4)

In Office 365 environments, organizations may grant Microsoft partners or resellers **delegated administrator permissions**.

By compromising a partner or reseller account, an adversary may be able to leverage existing delegated administrator relationships ...in order to gain administrative control over the victim tenant

A "nice" example (July 2023)



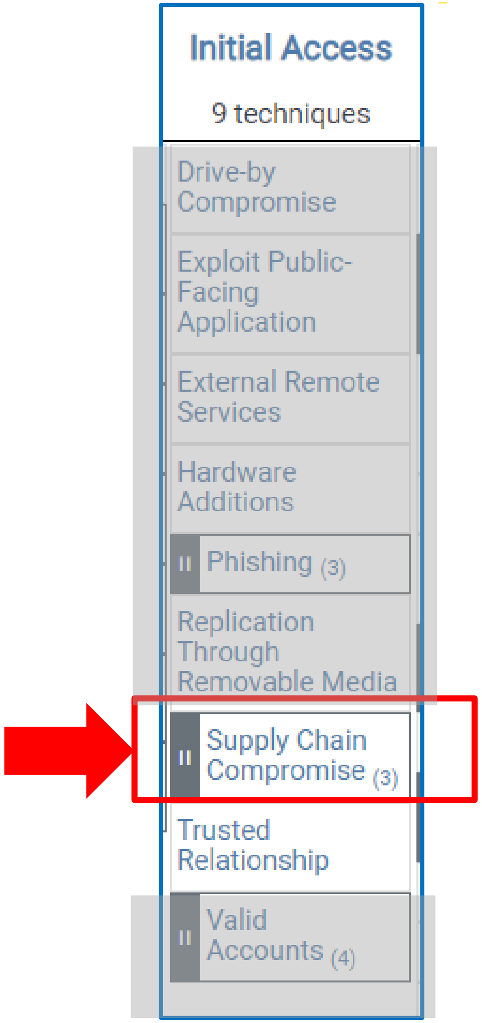
Microsoft lost its keys, and the government got hacked

Zack Whittaker @zackwhittaker / 4:05 PM GMT+2 • July 17, 2023

- China-backed hackers **stole a key that allowed them to stealthily break into dozens of email inboxes**, including those belonging to several federal government agencies.

- Hackers obtained a **Microsoft signing key** that was abused **to forge authentication tokens** that allowed the hackers’ access to inboxes as if they were the rightful owners

Supply Chain Compromise (I-a)

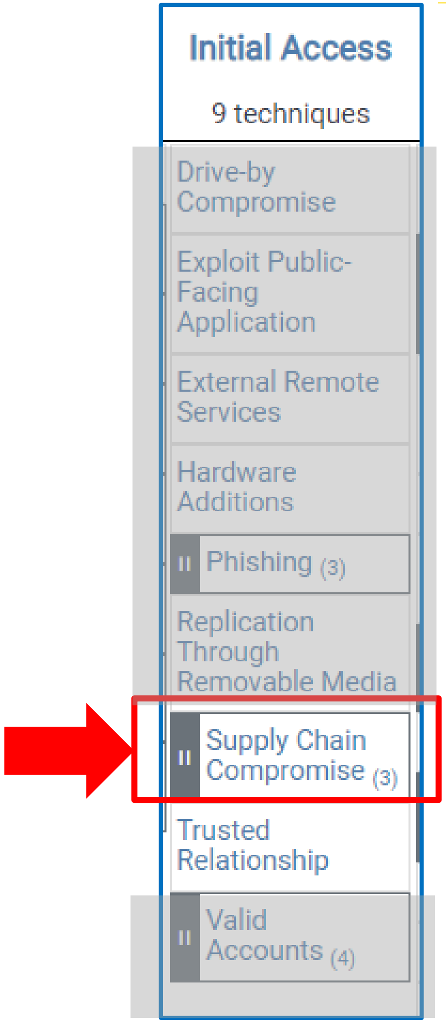


Adversaries may **manipulate products** or product **delivery mechanisms** prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at **any stage of the supply chain** including:

- Manipulation of **development tools**
- Manipulation of a **development environment**
- Manipulation of **source code repositories** (public or private)
- Manipulation of **source code** in open-source **dependencies**
- Manipulation of **software update/distribution** mechanisms
- Compromised/infected system images (multiple cases of removable media **infected at the factory**)
- Replacement of legitimate software with modified versions
- Sales of modified/counterfeit products to legitimate distributors
- Shipment interdiction

Supply Chain Compromise (I-b)



Initial Access

9 techniques

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (3)

Replication Through Removable Media

Supply Chain Compromise (3)

Trusted Relationship

Valid Accounts (4)

- Usually **malicious additions to legitimate software**.
- Usually distributed to a very broad set of consumers and then additional tactics to **specific** victims.
- Sometimes popular open source projects that are used as **dependencies** in many applications

SolarWinds

- Software for **security network monitoring**
- Adopted by **large** and **security-conscious organizations**
  - All five branches of the US military
  - State department, White House, NSA,
  - 425 of the Fortune 500 companies,
  - All five of the top five accounting firms
  - …

SolarWinds Compromise (December 2020)

- Software for **security network monitoring**
- Adopted by **large** and **security-conscious organizations**
  - All five branches of the US military
  - State department, White House, NSA,
  - 425 of the Fortune 500 companies,
  - All five of the top five accounting firms
  - …

- APT inserted malicious updates
- **18000** organizations installed the update
- **Evidence** of later attacks in **many hundreds** of them

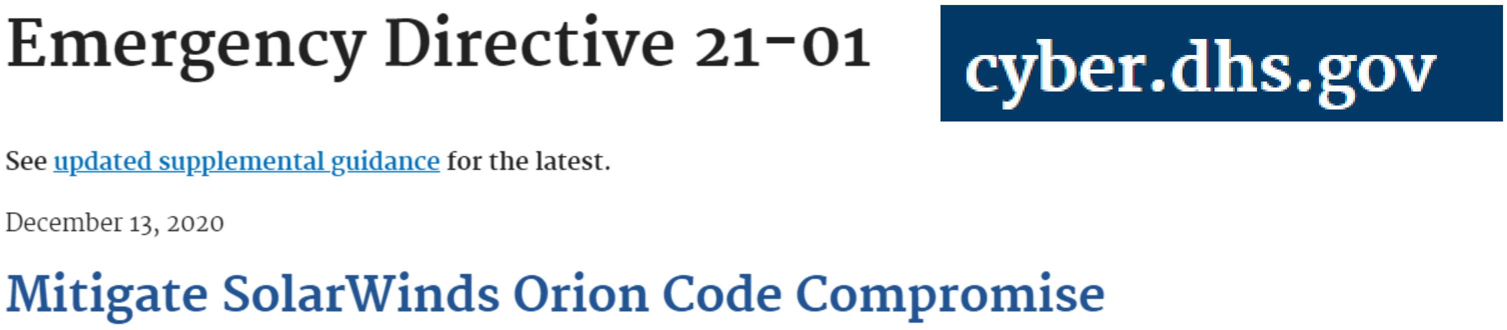
What happened (in a nutshell) (I)

1. **Intrusion** on SolarWinds
2. **Malicious update** on 18000 customers
3. Evidence of **intrusion** in many hundreds of them
   - Deployment of other malware + **persistence**

What happened (in a nutshell) (II)

3. Evidence of intrusion in many hundreds of them
    - Deployment of other malware + persistence
    - These included:
        - **FireEye**
            - Top of the tops security company
            - They alerted all the other organizations (no one had noticed)
        - **Microsoft** (alerted by FireEye)

Emergency Directive



Emergency Directive 21-01

cyber.dhs.gov

See updated supplemental guidance for the latest.

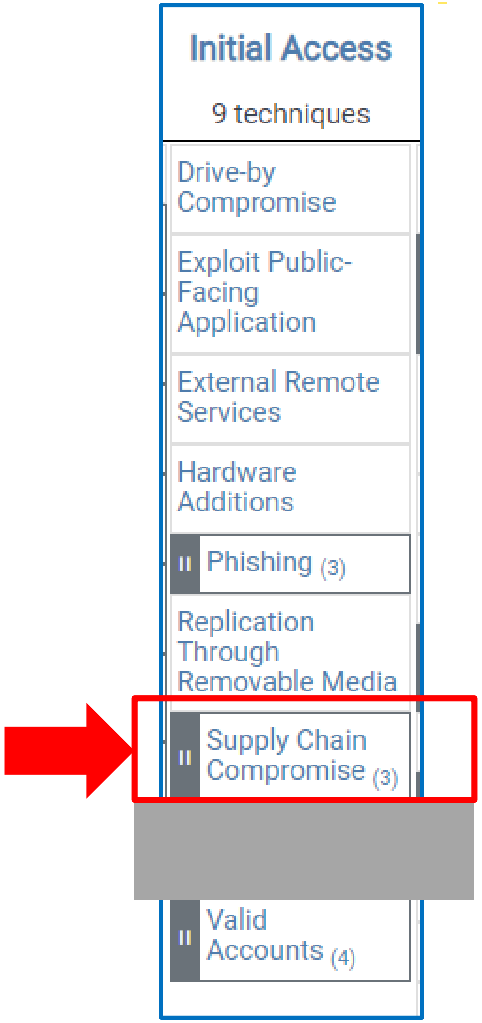
December 13, 2020

Mitigate SolarWinds Orion Code Compromise

- ❑ … **immediately disconnect or power down SolarWinds Orion products**
- ❑ …agencies are **prohibited** from (re)joining the Windows host OS to the enterprise domain
- ❑ **Block all traffic** external to the enterprise to and from hosts where any version of SolarWinds Orion software has been installed.

- ❑ How to clean up against persistence?

Keep in mind



Initial Access

9 techniques

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (3)

Replication Through Removable Media

Supply Chain Compromise (3)

[redacted]

Valid Accounts (4)

- ❑ Usually **malicious additions to legitimate software**.

- ❑ While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on **malicious additions** to **legitimate** software in software distribution or **update channels**.

Examples

1. Take a look at the "Supply Chain Compromise" examples on the companion website
2. Think a little about them
3. Change your job...

Supply Chain Compromise

Supply Chain Attacks: Why attractive

- Attack **one**, hit **many**

- Victims invariably have **lot of trust** in **a lot of** components:
  - **All** those that compose its **internal infrastructure**
  - **All** those that are used for **software development**

- Air gap does **not** defend

Supply Chain Defense: Why a nightmare (I)

- Do we even **know** our perimeter?
  - HW+SW Infrastructure: Network, Servers, Endpoints
    - Who manufactured our devices? Who sold them to us? Who installed them?
  - Internal Applications
    - Who built our website? Which platform does it run on? Which libraries?
    - And what about our mail server?
  - Software development tools and **libraries**
    - Which libraries have we used? Developed and maintaned by whom?
  - ...

Supply Chain Defense: Why a nightmare (II)

Supply chain compromise can take place at **any stage of the supply chain** including:

- ❑ Manipulation of **development tools**
- ❑ Manipulation of a **development environment**
- ❑ Manipulation of **source code repositories** (public or private)
- ❑ Manipulation of **source code** in open-source **dependencies**
- ❑ Manipulation of **software update/distribution** mechanisms
- ❑ Compromised/infected system images (multiple cases of removable media **infected at the factory**)
- ❑ Replacement of legitimate software with modified versions
- ❑ Sales of modified/counterfeit products to legitimate distributors
- ❑ Shipment interdiction

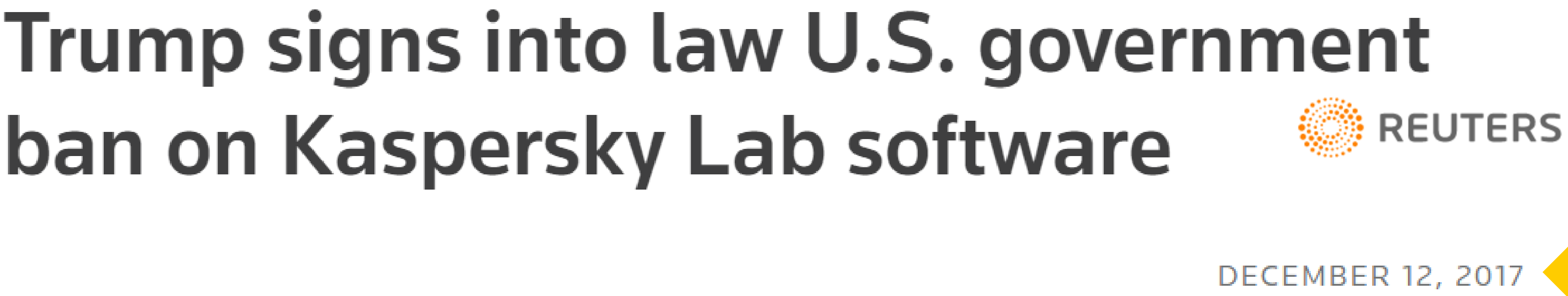
Supply Chain Defense (= cross your fingers)

- Best practice today:
  1. Understand risks
  2. Structure and manage relations with providers carefully

- Look at companion website

- Much easier said than done
- Point 2 has been applied for a long time in **critical non-cyber domains**

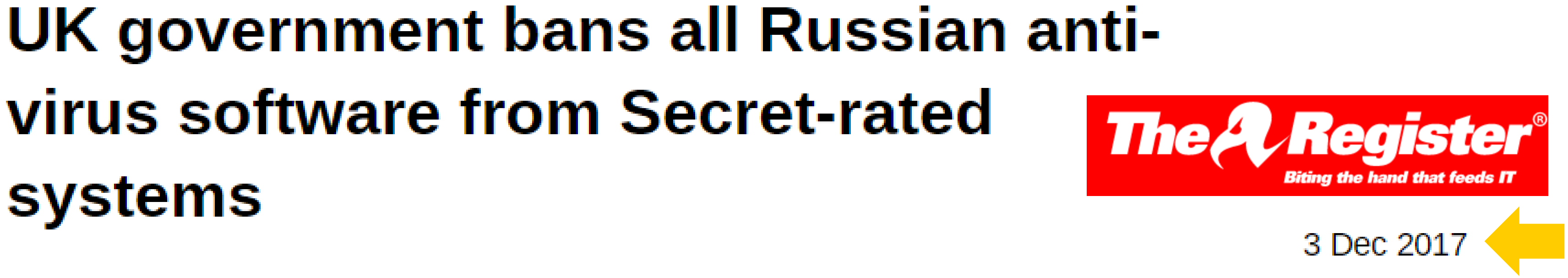
Note the timing



Trump signs into law U.S. government ban on Kaspersky Lab software

REUTERS

DECEMBER 12, 2017

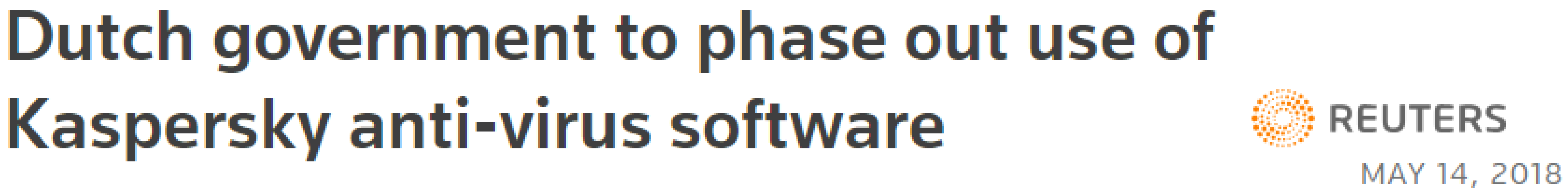


UK government bans all Russian anti-virus software from Secret-rated systems

The Register

Biting the hand that feeds IT

3 Dec 2017



Dutch government to phase out use of Kaspersky anti-virus software

REUTERS

MAY 14, 2018

Supply Chain Compromise: Keep in mind

- **Huge** problem
- No longer a theoretical possibility
- Will become more and more relevant