Supply Chain Attacks: Russian Criminal Enterprises as Unwelcome Guests in Your Network

Alex Urbelis, Neda Shaheen, and Jay Kramer

September 12, 2023

Crowell NCFTA ACC Association of Corporate Counsel NEW YORK CITY

Speakers

Alex Urbelis

Senior Counsel
Privacy & Cybersecurity
aurbelis@crowell.com

New York, NY
+1.212.895.4254

Neda Shaheen

Associate
Privacy & Cybersecurity / International Trade
nshaheen@crowell.com

Washington, DC
+1.202.624.2642

Jay Kramer

Managing Director
National Cyber-Forensics and Training Alliance
jkramer@ncfta.net

New York, NY
+1 347.300.5120

Agenda

This presentation will go through the following agenda:

- General background on how cybersecurity supply chain attacks operate;
- Identify the surprising origin of this types of cyberattacks;
- Discuss both the SolarWinds and MoveIT attacks;
- Address the adequacy of cyber liability insurance and the problem of third-party risk management
- Offer steps to prepare for, and mitigate the risk of, future supply chain attacks.

General Background on Cybersecurity Supply Chain Attacks

Crowell

Overview

- Supply chain attacks are also called value-chain or third-party attacks.
- Occurs by infiltrating trusted software or hardware systems, or through outside partner.
- By compromising a single supplier, bad actors can hijack the whole system.
- Bad actors often target unsecure networks, unprotected server infrastructures, and unsafe coding practices.
- Vendors can be unaware that their apps or updates are infected with malicious code.

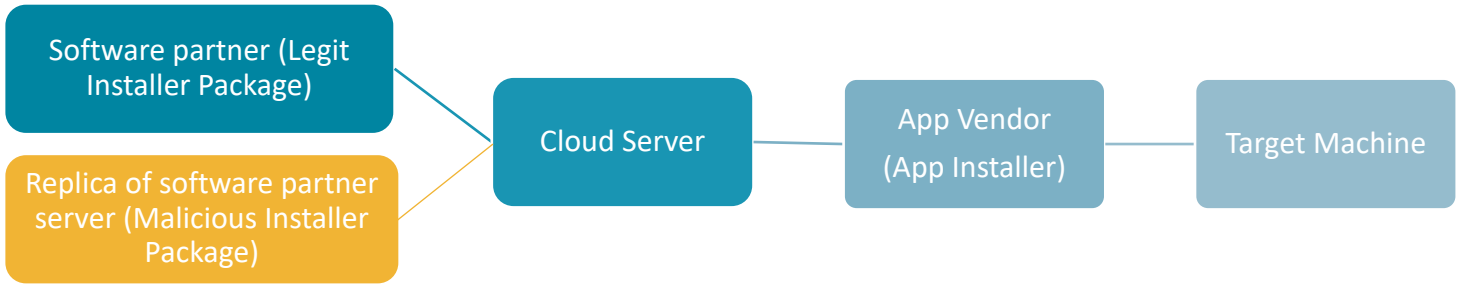
The ICT Supply Chain Is a Network

- The Information and Communications Technology (ICT) supply chain is a network of retailers, distributors, and suppliers that participate in the sale, delivery, and production of hardware, software, and managed services
- Widespread consequences for all sectors
- The ICT Supply Chain lifecycle has six phases. At each phase, there is risk.

Source: CISA & NIST, Defending Against Software Supply Chain Attacks

Multi-Tier Attacks

- In a multi-tier attack, attackers compromise the shared infrastructure between the software vendor and one of its partners, making an app's legitimate installer the unsuspecting carrier of a malicious code.
- For example, in a multi-tier attack against Microsoft:
  - Attackers recreated the software partner's infrastructure on a replica server. They copied and hosted all MSI files, including font packages, in the replica sever.
  - The attackers decompiled and modified one MSI file, a font pack, to add the malicious payload with the coin mining code.
  - Using an unspecified weakness, the attackers influences the download parameters used by the app. The parameters included a new download link that pointed to the attacker server.
  - As a result, the link used by the app to download MSI font packages pointed to a domain name registered with a foreign registrar and pointed to a server hosted on a popular cloud platform provider.
  - The app installer from the app vendor, still legitimate and not compromised, followed the hijacked links to the attackers' replica server instead of the software partner's server.



Source: Microsoft, Attack inception: Compromised supply chain within a supply chain poses new risks

Origin of Supply Chain Attacks

Crowell

Supply Chain Attacks Are Not New

- SolarWinds increased awareness on supply chain hacks. However, these attacks are not new.
  - 1970s: First computer worm was created. First cybersecurity effort to eliminate it was also created.
  - 1980s: First commercial anti-virus product is available
  - 1990s: The internet goes public. Firewalls and antivirus programs are produced at mass scale.
  - 2000s: Threats diversify and multiply. First supply chain attacks start.
  - 2020s: The industry grows at the speed of light.

Ongoing Process | Yossi Kotler

Rewind: NotPetya Ukraine, 2017

- Ukraine as proving ground for cyberattacks
- Tax prep software – M.E. Doc compromised
- Remote code exec + creds hunt in RAM
- Relied on EternalBlue, an NSA SMB exploit
- Spread around the world and damage, not money, seemed to be the motivation

Identity / Nivesh Trivedi

Counterfeit Cisco Products, United States, 2008

- Supply Chain attacks can also happen on hardware.
- Sold counterfeit Cisco routers to the U.S. Military.
- Discovered 3,500 counterfeit Cisco Systems network components.
- Opened a hardware backdoor into U.S. government systems and impacted critical national infrastructure

Coy and Counterfactual / Terry Castle

Examples of Recent Supply Chain Attacks

- 2017: NotPetya
- 2017: Altair Technologies
- 2017: Piriform
- 2017: ME Doc
- 2018: VestaCP
- 2018: PDF Editor App
- 2018: Browsealoud
- 2018: Python programming language
- 2018: Copay (now BitPay)
- 2019: Agma Cryptocurrency
- 2019: ASUSTek
- 2020: U.S. Government program for low-income Americans
- 2020: NetBeans Project
- 2020: Able Desktop
- 2020: Aisino
- 2020: WIZVERA VeraPort
- 2020: Solar Winds
- 2020: Vietnam VCGA
- 2020: Twilio
- 2021: Mimecast
- 2021: Stock Investment Platform
- 2021: BigNox
- 2021: 35 Systems,. Including Microsoft, Apply, PayPal, Shopify, Netflix, Yelp, Tesla, and Uber, etc.
- 2021: MonPass
- 2021: Xcode
- 2021: Click Studios
- 2021: Code Gov
- 2021: Ledger (Nano X Wallet)
- 2021: Myanmar Presidential Website
- 2021: SYNNEX
- 2021: SushiSwap MISO Cryptocurrency
- 2021: npm 'coa' and 'rc' packages
- 2022: OSS Projects (e.g. Amazon cloud development kit, Javacript, and Node.js.)
- 2022: Samsung
- 2022: NPM node.ipc module
- 2022: IconBurst
- 2022: React and QT
- 2022: PyPi, Linux
- 2022: TA569, national and regional newspapers

The SolarWinds Hack: Elegance and Efficacy

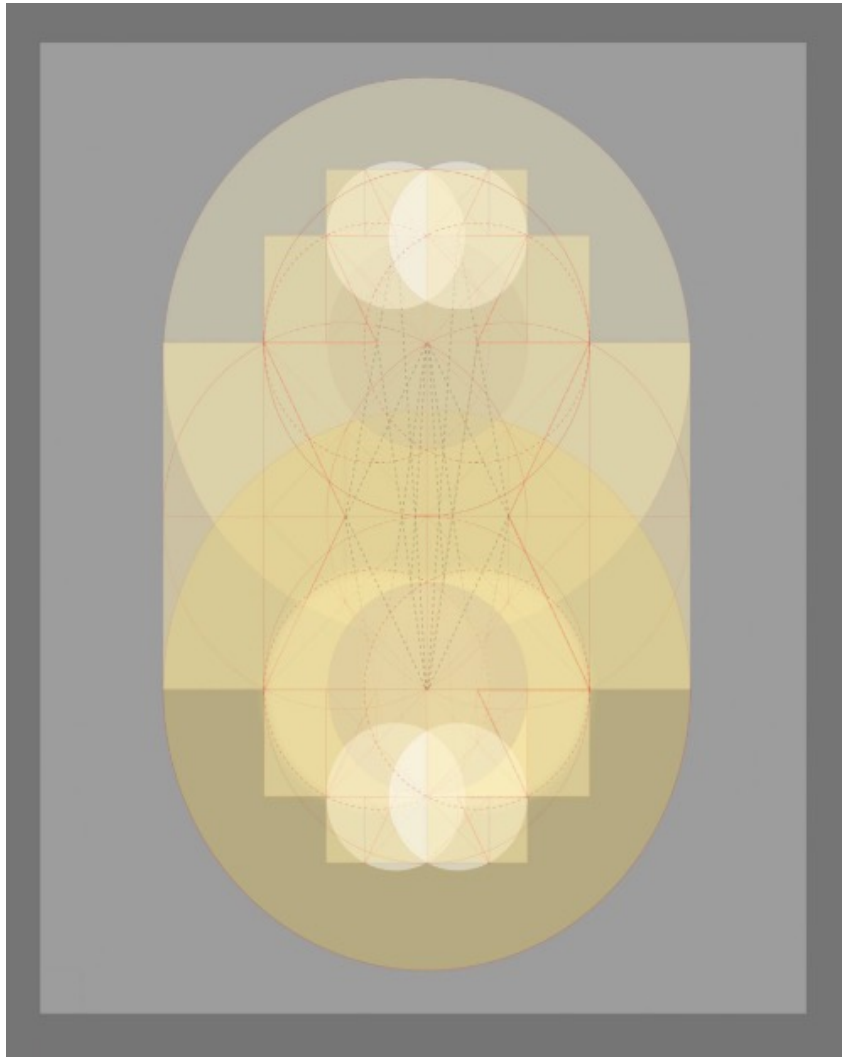
The SolarWinds Hack: A Supply Chain Nightmare

- Malicious code inserted into software
- Propagated through a software update
- Created a backdoor into 18,000 unsuspecting companies and agencies
- Entirely unnoticed
- Elegant, effective, eminently historical

Computer Hacker | Richard Arfsten

Who is SolarWinds?

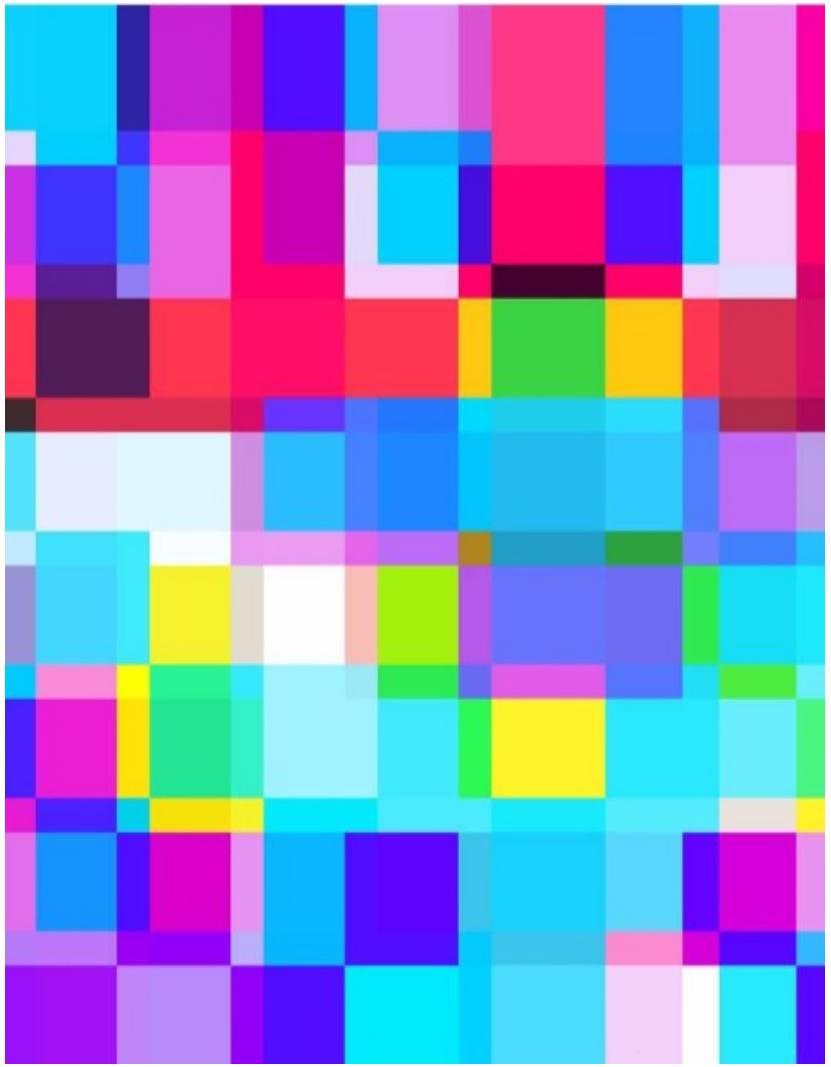
- Texas-based software company
- IT administration software: Orion
- Allows the management of hundreds or thousands of servers / machines
- Management of devices requires privileged access to those devices



Polarity, Connectivity | Duc Ly

The Numbers

- 18,000 companies / agencies downloaded
- 100 or so actually impacted / breached
- Microsoft, FireEye, Qualys, Chevron, Intel, Cisco, CISA, and other US federal agencies
- Permitted lateral movement amongst networks
- Also could have planted malware / backdoors



After Piet Mondrian | Andrea Pallang

Back to SolarWinds: The Attack Vectors

- Accessed production code repository
- Maliciously modified source code
- Used domain names to identify targets
- Mimicked / piggybacked on Orion protocols
- Effective anti-forensics – a clean-up job

Ducky Attacks the HW Bush | Ken Vrana

The Test Balloon

- 2019 – one snippet of innocuous code
- Tested to see if processor was 32- or 64-bit
- Put this code into the production version
- Code as pushed out to SolarWinds clients
- Proof of concept that more malicious code could permit a full-scale supply chain attack

Golf Painting | Trevisan Carlo

Getting to work…

- 5 months later – February 2020
- Developed an implant backdoor system
- Source code audited before compiled
- While compiling, swapped in malicious file
- Last possible second; unclear how updates to actual source code were ported to temp file

Roll Up Your Sleeves | Stefan Smit

The Packaging Matters

- Once compiled, the binary files are distributed from SolarWinds and with their packaging
- Normal techniques to identify attacks would fail
- Hashes of the malicious update were legit
- The malicious files with the payload were then distributed through normal update channels

Encombrants 3 | Sylvain Fornaro

Back to Solar Winds

- FireEye (now Mandiant) informs SolarWinds they found malicious code when they decompiled Orion
- The media was onto the story
- SolarWinds lawyers up
- Very concerned about protecting privilege
- Lawyers then hire CrowdStrike for forensics

Lebensstufen I | Andre Schulze

Attribution Points to Russia

- 3,500 lines of encrypted code
- Very elegantly written and efficient
- No indications of origin; nothing re-used; no fonts or special characters within the code
- Highly efficient anti-forensic activities
- U.S. government attributes attacks to Russia's Foreign Intelligence Service (SVR)

Who Are You Mister Putin | Maxim Fomenko

Legal and Policy Response

- Pres. Biden issues Exec. Order to strengthen the government's cybersecurity practices
- Government removes barriers to threat intel sharing and focuses on software supply chain vulnerabilities
- SolarWinds stock drops 40%
- Shareholders sue the company and its officers under the Exchange Act
- MTD denied; case proceeding, even re CISO

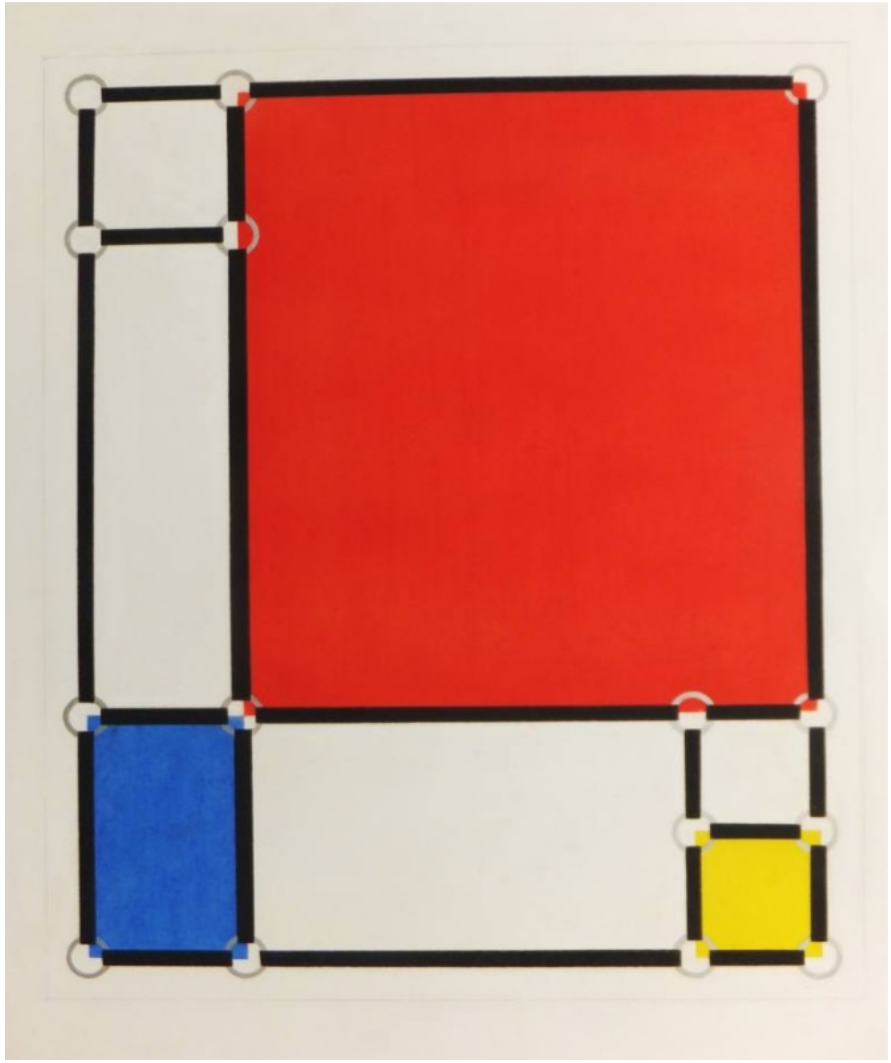
Court Artwork | Bruno Schiaraffia

The MOVEit Hack and Supply Chain Risks

Crowell

What is MOVEit?

- MOVEit is a managed file transfer software product.
- Produced by Progress Software
- Encrypts files and uses file transfer protocols such as FTP or SFTP to transfer data.
- Used by organizations to ship large amounts of sensitive data.



Secured Mondrian 5 Drawing | Walter Fydryck

The MOVEit Breach: A Devastating Zero-Day Vulnerability

- The MOVEit Breach started on May 27, 2023.
- CL0P, the Russian ransomware group, claimed responsibility for the attack.
- Vulnerability was found in Progress Software's managed file transfer (MFT) solution known as MOVEit Transfer.

The Fool From Point Zero | Franck de las Mercedes

What Is MOVEit?

- It was caught relatively quickly and some organizations were able to deploy a patch.
- Affected at least 122 organizations and roughly 15.5 million people.
- No industry escaped the consequences

Eternally affected / Dags Vidulejs

What happened next?

- ClOP started publishing, updating, and leaking
- We still don't know the number of those affected (estimates)
- Negotiations with ClOP went on behind the scenes.
- Many companies do not know if they have been impacted. If company was the counter-party, there would be no visibility unless impacted company told them.
- There is no affirmative obligation to go public with whether you've been impacted.

REUTERS® World Business Markets Sustainability More

Alexander Urbelis, senior counsel with New York-based law firm Crowell & Moring, which has helped victims gauge their exposure to the hackers' dragnet, said extraordinarily slow download speeds from the hackers' creaky darknet website "made it all but impossible for anyone" - whether well-intentioned or otherwise - "to access the stolen data."

What happens next
Tavi Weisz

Cyber Liability Insurance and The Problem of Third-Party Risk Management

Crowell

What is Cyber-Liability?

- An insurance policy that provides businesses with a combination of coverage options to help protect the company from data breaches and other cyber security issues.
- Cyber Liability Insurance covers things like–
  - Data breaches
  - Cyber attacks on data held by third parties
  - Network breaches
  - Cyber attacks that occur anywhere in the world (not only in the United States)
  - Terrorist acts

Covered by Irregularity #08/ Tomasz Chichowski

Underwriting a Cyber Liability Insurance Policy

- Underwriting is very intense.
- Insurance companies assess client risk, evaluate exposure, and model losses, including the cost to recover from a data breach, ransomware attack, or other malicious cyber activity.
- This has been a big change in the last few years.

Useless Words – Edition of 3 / Kasia Derwinska

Third-Party Cyber Liability Insurance

- Covers expenses for businesses responsible for clients' online security and data.
- Third-Party Cyber Liability Insurance can help pay for–
  - Lawyers' fees
  - Settlements
  - Judgments
  - Other court costs (e.g. witness fees, docket fees, etc.)

Time to Pay the Piper / Jim Harris

Cyber Liability Insurance and Acts of War

- *This is still an open question*.
- Insurers argue that under the act of war doctrine, losses arising from cyberattacks perpetrated by state actors are not covered under cyber liability insurance policies.
- The New Jersey Superior Court recently found that a "hostile/warlike action" exclusion clause should not be applied to a cyberattack on a non-military company
- Consider the impact on global supply chains.
  - In MOVEit, Cl0p breached members or the defense industrial base. Is that an act of war?

Before Storm / Gregor Ziolkowski

Prepare for and Mitigate the Risk of Future Supply Chain Attacks.

Crowell

Supply Chains Are Uniquely Vulnerable

- Organizations are uniquely vulnerable to software supply chain attacks for two major reasons:
  - First, many third-party software products require privileged access; and
  - Second, many third-party software products require frequent communication between a vendor's network and the vendor's software product located on customer networks.

CISA Recommendations

- CISA Recommendations to Customers
  - Actions to Prevent Acquiring Malicious or Vulnerable Software
  - Actions to Mitigate Deployed Malicious or Vulnerable Software
  - Actions to Increase Resilience to a Successful Exploit

- CISA Recommendations to Software Vendors
  - Actions to Prevent Supplying Malicious or Vulnerable Software
  - Actions to Mitigate Post-Deployment Malicious or Vulnerable Content
  - Actions to Increase Resilience in the Software Development Process
  - Considerations to Implementing a Secure Software Development Framework

CSRB Recommendations

- In a report by the Cyber Safety Review Board, they provide recommendations organized by four key themes:
  - Strengthen identity and access management (IAM);
  - Mitigate telecommunications and reseller vulnerabilities;
  - Build resiliency across multi-party systems with a focus on business process outsourcers (BPOs); and
  - Address law enforcement challenges and juvenile cybercrime.

- The Board is responsible for identifying improvements for cybersecurity and making independent, strategic, and actionable recommendations to the President

Source: CISA, Review of the Attacks Associated with LAPSUS$ and Related Threat Groups

Crowell Recommendations

- These attacks compromise the vendor so a multi-layered defense is critical.
  - Focus on people, process, and technology. Process includes vetting, assurance, identity and access management, active monitoring, escalation, etc.
  - Foster cross-sector collaboration and information sharing with trusted professionals, such as NCFTA
  - Provide regular cybersecurity training.
  - Have a prepared responsible plan and procedures in place to mitigate unique challenges (e.g. ransomware, extortion, and harassment).

Source: CISA, Review of the Attacks Associated with LAPSUS$ and Related Threat Groups

Questions?

Thank you

crowell.com