Kevin McPeak CISSP ITILv3
@kevin_mcpeak
linkedin.com/in/kevinmcpeak

Managing Your Supply Chain Security:

Understanding Supply Chain Security Risks

Preventing Second Hand or Counterfeit Device Components

Agenda

- Overview of Presentation Goals: Stimulate Thought and Define Areas for Further Research
- Defining Supply Chain Resiliency, Security, Agility & Sustainability
- Developing and Maturing your Supply Chain Security Program
- Emerging Topic: Using Blockchain Security in your Supply Chain
- Emerging Topic: Leveraging the Power of a Software Bill of Materials (SBoM)
- Emerging Topic: Understanding the Google SLSA (pronounced “salsa”) Model
- Technical Supply Chain Security Concerns via Examples: Automotive Software (As-Is and Emerging Driverless Cars); Medical Technology; Traditional IT Infrastructure vs WFH/WFA IT Infrastructure; Ubiquitous IoT / IoE
- Technical Overview: Preventing Counterfeit Components within your Manufacturing Supply Chain
- Understanding Your Supply Chain Dependencies: How Cyber Attacks Directed Against Logistics and Fuel Suppliers Can Massively Disrupt your Operations:
  - Example #1: Maersk
  - Example #2: FedEx
  - Example #3: Colonial Pipeline (Deep Dive on What Happened)
- Conclusion/Questions

Supply Chain:
Resiliency, Security, Agility & Sustainability

NIST

Search CSRC | ≡ CSRC MENU

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

SP 800-161 Rev. 1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Date Published: May 2022

Planning Note (5/5/2022):

The guidance from Appendix F, "Response to Executive Order 14028's Call to Publish Guidelines for Enhancing Software Supply Chain Security," is available at NIST's dedicated EO 14028 website.

Author(s)

Jon Boyens (NIST), Angela Smith (NIST), Nadya Bartol (Boston Consulting Group), Kris Winkler (Boston Consulting Group), Alex Holbrook (Boston Consulting Group), Matthew Fallon (Boston Consulting Group)

Abstract

Organizations are concerned about the risks associated with products and services that may potentially contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain. These risks are associated with an enterprise's decreased visibility into and understanding of how the technology they acquire is developed, integrated, and deployed or the processes, procedures, standards, and practices used to ensure the security, resilience, reliability, safety, integrity, and quality of the products and services.

This publication provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations. The publication integrates cybersecurity supply chain risk management (C-SCRM) into risk management activities by applying a multilevel, C-SCRM-specific approach, including guidance on the development of C-SCRM strategy implementation plans, C-SCRM policies, C-SCRM plans, and risk assessments for products and services.

Keywords

acquire; C-SCRM; cybersecurity supply chain; cybersecurity supply chain risk management; information and communication technology; risk management; supplier; supply chain; supply chain risk assessment; supply chain assurance; supply chain risk; supply chain security

DOCUMENTATION

Publication:
SP 800-161 Rev. 1 (DOI)
Local Download

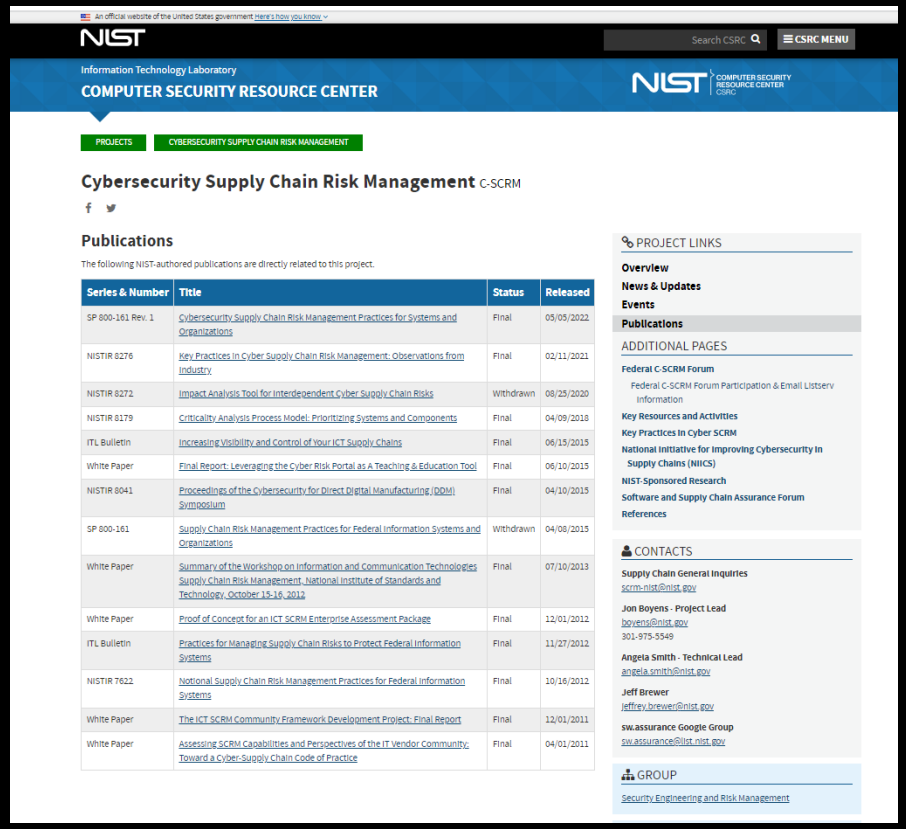
Supplemental Material:
EO 14028: Software Security in Supply Chains (web)
NIST's Cyber Supply Chain Risk Management Program (other)
NIST news article (web)

Document History:
02/04/20: SP 800-161 Rev. 1 (Draft)
04/29/21: SP 800-161 Rev. 1 (Draft)
10/28/21: SP 800-161 Rev. 1 (Draft)
05/05/22: SP 800-161 Rev. 1 (Final)

TOPICS

Security and Privacy
acquisition; cybersecurity supply chain risk management

Laws and Regulations
Executive Order 14028



NIST

Search CSRC | ≡ CSRC MENU

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PROJECTS | CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT

Cybersecurity Supply Chain Risk Management C-SCRM

Publications

The following NIST-authored publications are directly related to this project.

Series & Number	Title	Status	Released
SP 800-161 Rev. 1	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	Final	05/05/2022
NISTIR 8276	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	Final	02/11/2021
NISTIR 8272	Impact Analysis Tool for Interdependent Cyber Supply Chain Risks	Withdrawn	08/25/2020
NISTIR 8179	Criticality Analysis Process Model: Prioritizing Systems and Components	Final	04/09/2018
ITL Bulletin	Increasing Visibility and Control of Your ICT Supply Chains	Final	06/15/2015
White Paper	Final Report: Leveraging the Cyber Risk Portal as A Teaching & Education Tool	Final	06/10/2015
NISTIR 8041	Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium	Final	04/10/2015
SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	Withdrawn	04/08/2015
White Paper	Summary of the Workshop on Information and Communication Technologies Supply Chain Risk Management, National Institute of Standards and Technology, October 15-16, 2012	Final	07/10/2013
White Paper	Proof of Concept for an ICT SCRM Enterprise Assessment Package	Final	12/01/2012
ITL Bulletin	Practices for Managing Supply Chain Risks to Protect Federal Information Systems	Final	11/27/2012
NISTIR 7622	National Supply Chain Risk Management Practices for Federal Information Systems	Final	10/16/2012
White Paper	The ICT SCRM Community Framework Development Project: Final Report	Final	12/01/2011
White Paper	Assessing SCRM Capabilities and Perspectives of the IT Vendor Community: Toward a Cyber-Supply Chain Code of Practice	Final	04/01/2011

PROJECT LINKS

Overview
News & Updates
Events
Publications

ADDITIONAL PAGES

Federal C-SCRM Forum
Federal C-SCRM Forum Participation & Email Listserv Information
Key Resources and Activities
Key Practices in Cyber SCRM
National Initiative for Improving Cybersecurity in Supply Chains (NIICS)
NIST-Sponsored Research
Software and Supply Chain Assurance Forum
References

CONTACTS

Supply Chain General Inquiries
scrm-nist@nist.gov

Jon Boyens - Project Lead
boyens@nist.gov
301-975-5549

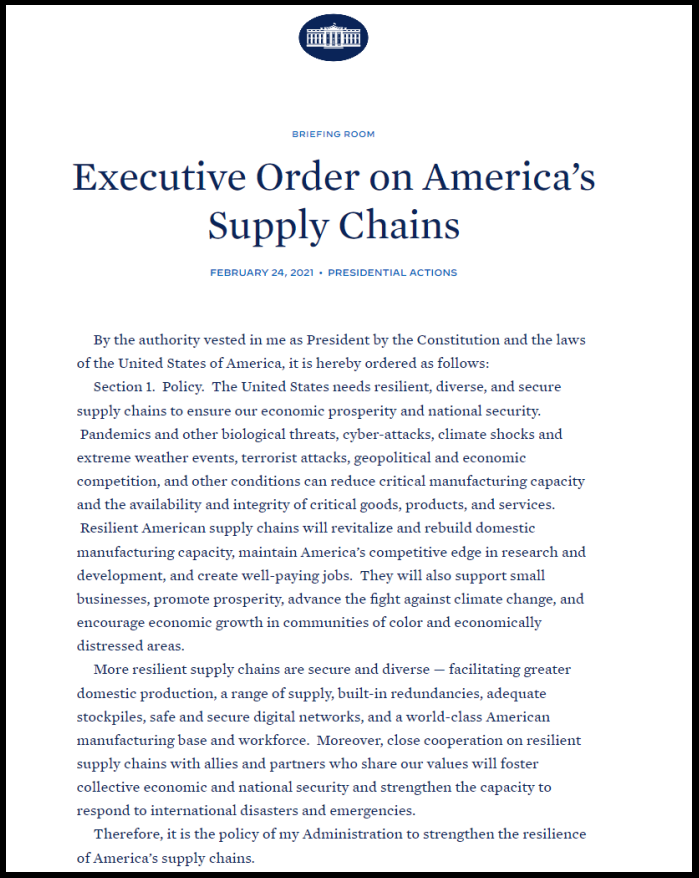
Angela Smith - Technical Lead
angela.smith@nist.gov

Jeff Brewer
jeffrey.brewer@nist.gov

sw.assurance Google Group
sw.assurance@list.nist.gov

GROUP

Security Engineering and Risk Management



BRIEFING ROOM

Executive Order on America's Supply Chains

FEBRUARY 24, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. Pandemics and other biological threats, cyber-attacks, climate shocks and extreme weather events, terrorist attacks, geopolitical and economic competition, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical goods, products, and services. Resilient American supply chains will revitalize and rebuild domestic manufacturing capacity, maintain America's competitive edge in research and development, and create well-paying jobs. They will also support small businesses, promote prosperity, advance the fight against climate change, and encourage economic growth in communities of color and economically distressed areas.

More resilient supply chains are secure and diverse — facilitating greater domestic production, a range of supply, built-in redundancies, adequate stockpiles, safe and secure digital networks, and a world-class American manufacturing base and workforce. Moreover, close cooperation on resilient supply chains with allies and partners who share our values will foster collective economic and national security and strengthen the capacity to respond to international disasters and emergencies.

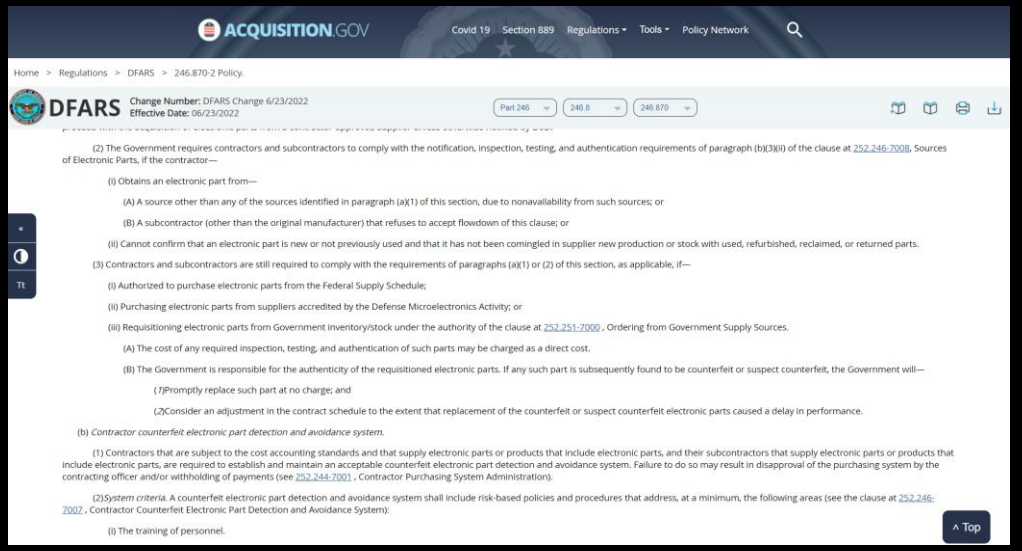
Therefore, it is the policy of my Administration to strengthen the resilience of America's supply chains.

Sources: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications

Developing & Maturing Your Supply Chain Security Program

A strong product supply chain supplier base (including ODMs, OEMs, component manufacturers, BIOS and software providers) is critical to your success.

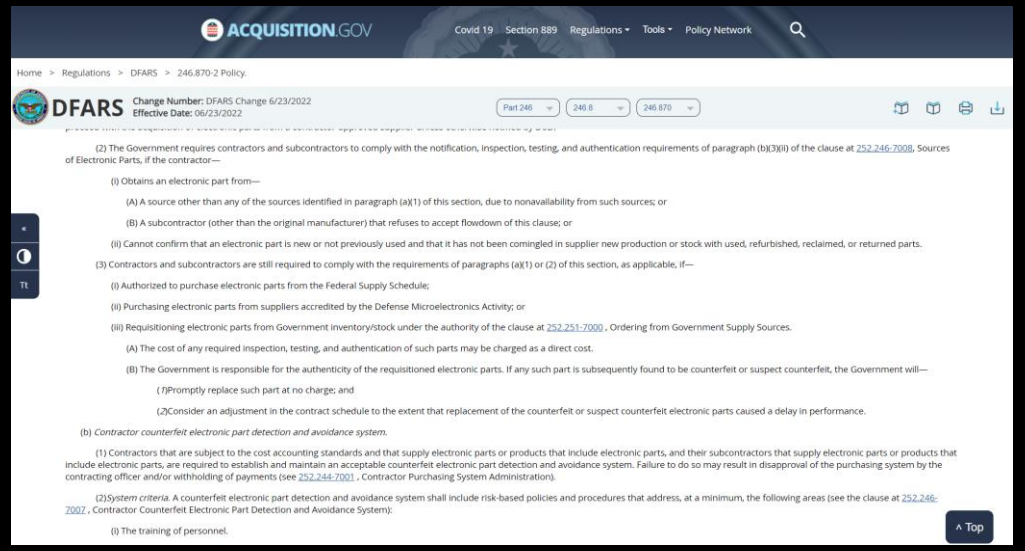
- Develop a process for qualifying your core suppliers which includes formally evaluating them on a recurring cadence that you define
- Develop a process to thoroughly assess new suppliers
- Develop plans to adjust supply chains to minimize impact, to be able to work with your suppliers to rapidly identify and address issues
- Develop a strategy and process to replace suppliers if issues remain unresolved



Developing & Maturing Your Supply Chain Security Program (Continued)

Manage your supply chain risk through a documented and auditable supply chain security program. Focus on your suppliers of intelligent components, ODMs, OEMs, and repair service providers that could impact your downstream customers' security.

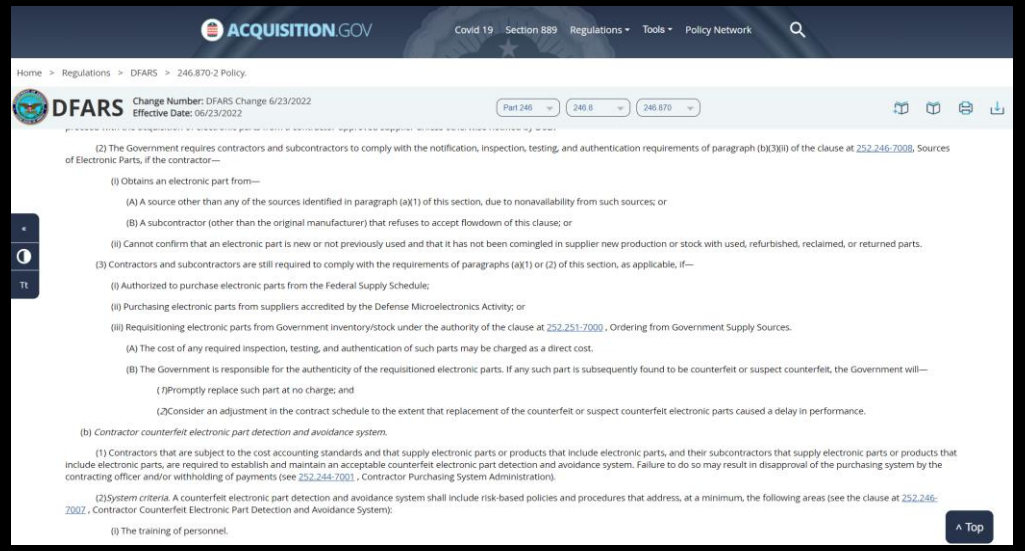
- Proactively and continually reviews your sourcing requirements to ensure that you keep up with - and stay ahead of - trends and vulnerabilities as they arise in the technology marketplace.
- Set supplier security expectations. Have frank discussions that the increasingly complex nature of the modern global supply chain is optimized for cost reduction and speed of delivery. This creates an opportunity for malevolent actors to conduct sophisticated attacks. For example, manufacturing sabotage, counterfeit components and sub-components, transit fraud, and theft are areas that should be of great concern for you and your suppliers.



Developing & Maturing Your Supply Chain Security Program (Continued)

Work diligently to prevent counterfeit components from contaminating your Supply Chain.

- Trace serial numbers or similar identifiers that are stamped or embedded during downstream manufacturing.
- For software components, work closely with your software vendors to ensure that only accurate, non-counterfeit software is ever installed on your systems.
- Once loaded, software vendors should provide methods to ensure that installed software is correct and has not been counterfeited.



Emerging Topic: Using Blockchain Security in your Supply Chain

Blockchain-based technologies can simplify supply chain management by making everything more transparent. This can occur when blockchain is used to create a single source of information about products in a supply chain via a global ledger. To do so, each component has to have its own entry on the blockchain, which gets tracked over time.

- Authorized companies can update the status of each component in real-time.
- Highly Qualified Results: Once you receive your manufactured device, you can trace every component back to its manufacturer.

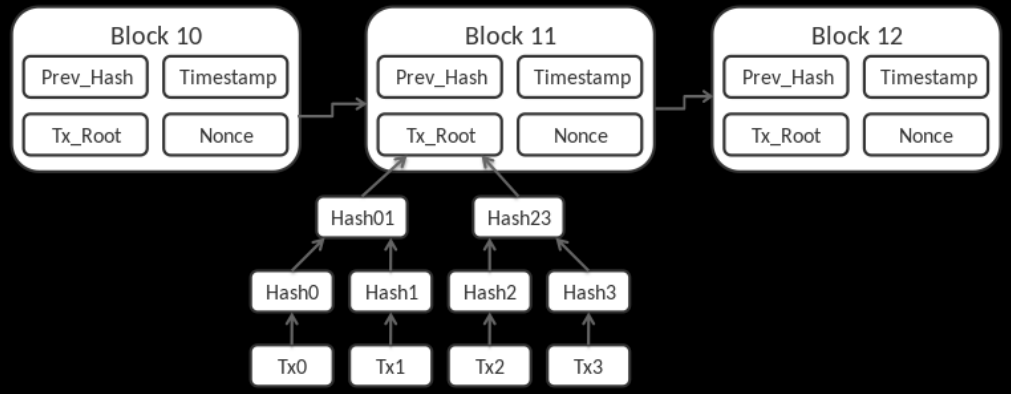


Image Source: https://commons.wikimedia.org/wiki/File:Bitcoin_Block_Data.svg

Emerging Topic: Using Blockchain Security in your Supply Chain

Theoretically, you could potentially trace the supply chain all the way back to the mines where the raw materials originate from.

Companies can use blockchain within their supply chain as a single source of truth to manage and monitor risks and to track delivery status of orders.

Likewise, companies can also manage and pay for supply chain components after each security test is completed.

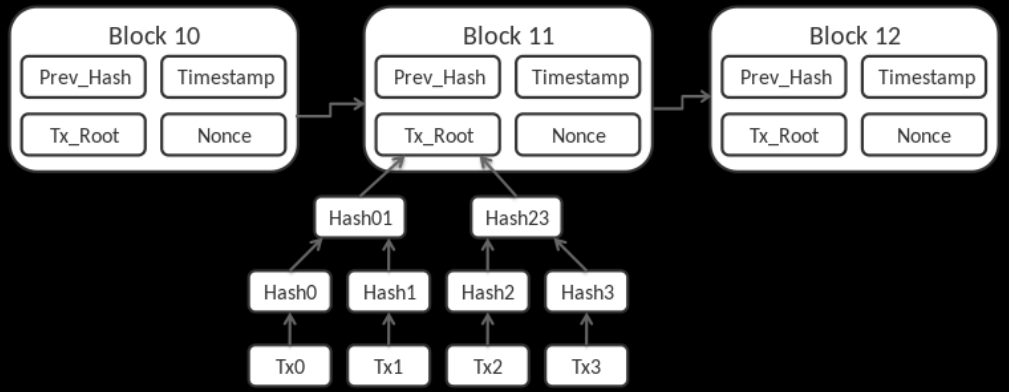


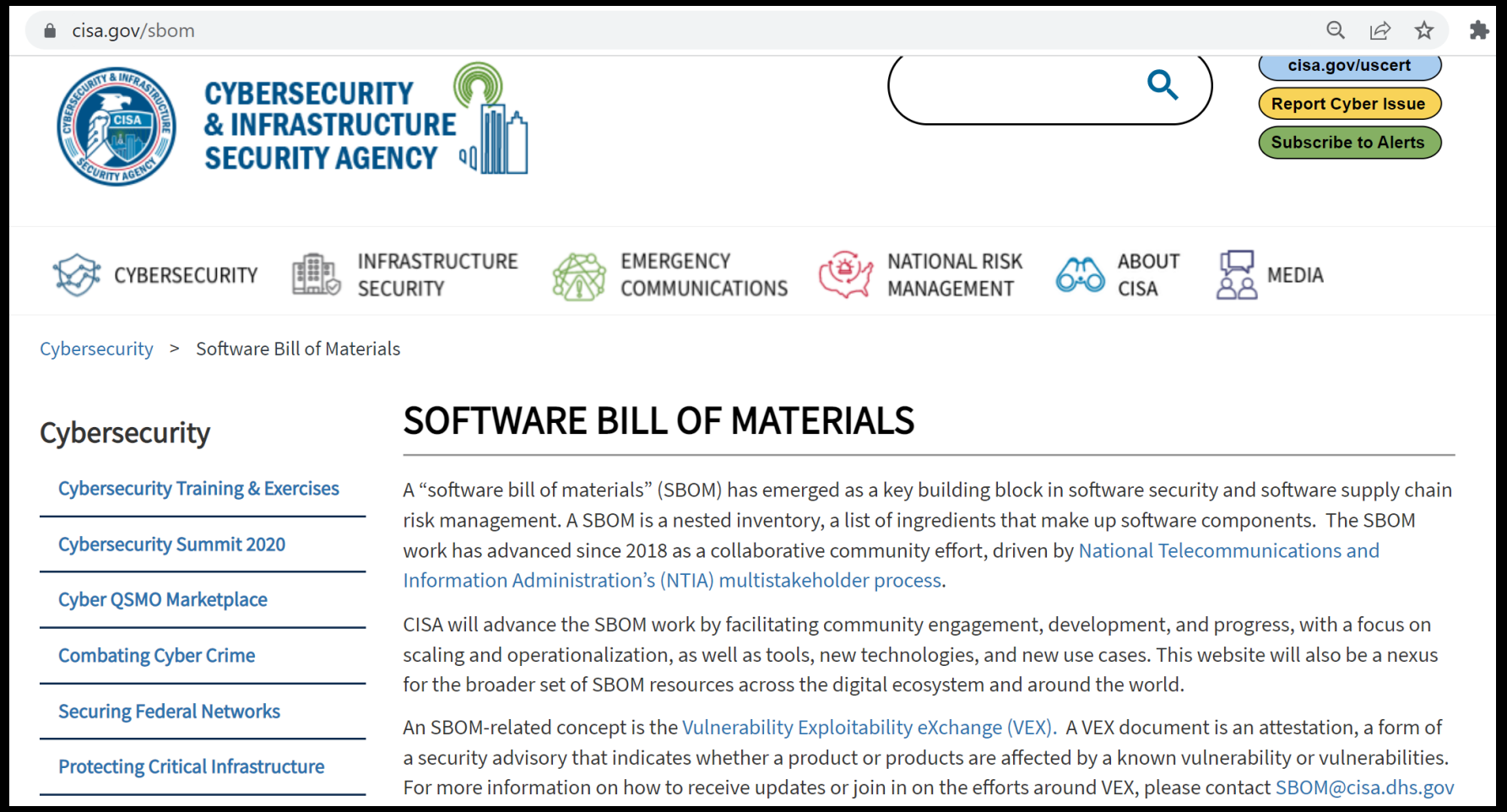
Image Source: https://commons.wikimedia.org/wiki/File:Bitcoin_Block_Data.svg

Leveraging the Power of SBoM

Software Bill of Materials (SBoM)

CISA definition:

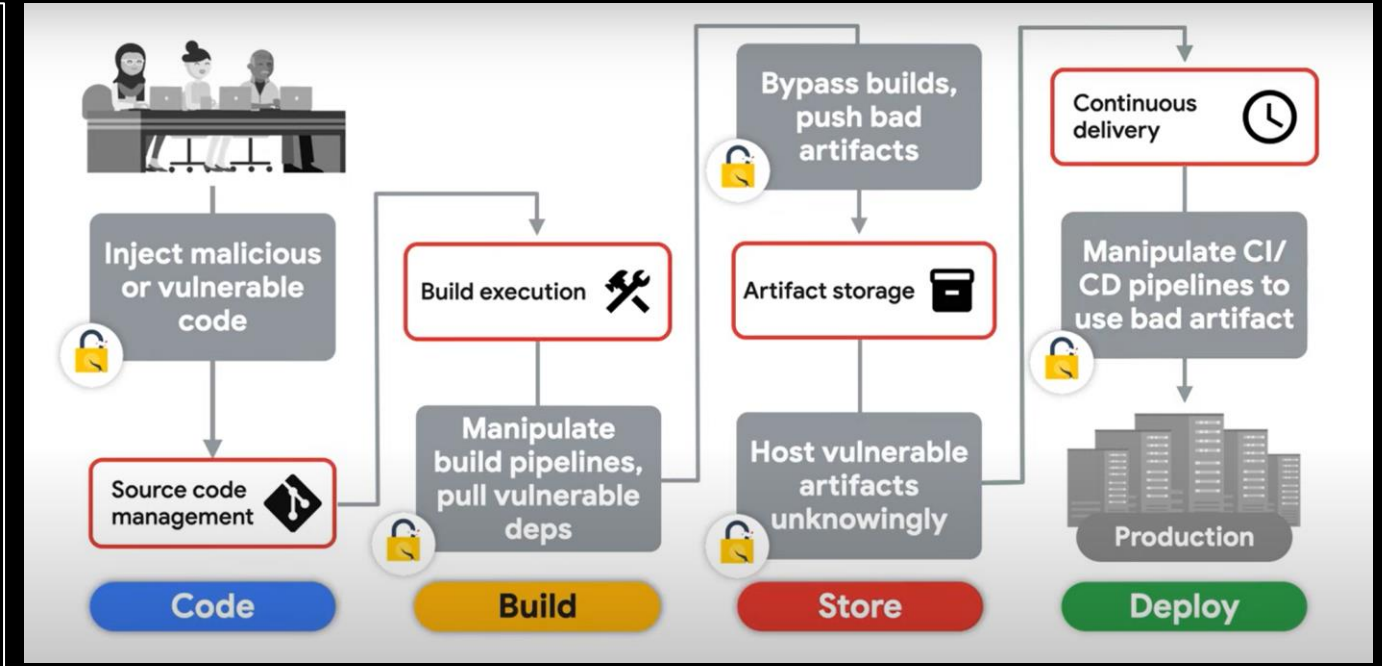
a “nested inventory” (a list of ingredients) that make up software components



Understanding the Google SLSA Model

The Google approach, known as Supply Chain Levels for Software Artifacts (SLSA, pronounced "salsa"), is an end-to-end framework for ensuring the integrity of software artifacts throughout the software supply chain.

- It is inspired by Google's internal "Binary Authorization for Borg" which has been in use for the past 8+ years and is mandatory for all of Google's production workloads.
- The goal of SLSA is to improve the state of the industry, particularly open source, to defend against the most pressing integrity threats.
- **With SLSA, consumers can make informed choices about the security posture of the software they consume. In short, SLSA helps to protect against common supply chain attacks.**

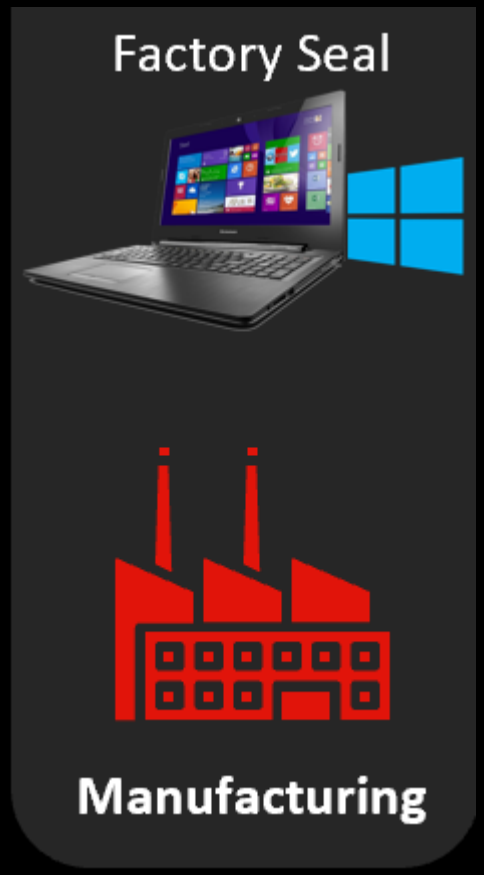


Sources: https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html
https://www.youtube.com/watch?v=Dg-hD4HHKT8

Technical Supply Chain Security Concerns: Real-World Examples

- **Automotive Software**
  - As-Is
  - Emerging Driverless Cars
  - Example: TPISR (3rd Party Information Security Requirements) from the Auto Industry Action Group (AIAG)
- **Medical Technology**
  - On-Premise (Hospital Equipment)
  - Patient Embedded
- **Traditional IT Infrastructure vs WFH/WFA IT Infrastructure**
  - Similarities
  - Differences
- **Ubiquitous IoT and IoE**

Preventing Counterfeit Components within your Manufacturing Supply Chain



WHITE PAPER

Computing System Manufacturing
Supply Chain Security

intel | Goldman Sachs

The Next Security Frontier: Taking the Mystery Out of the Supply Chain

Understanding the Strategic Importance of Transparency in the Computing Ecosystem

Authors

Michael Mattioli
Goldman Sachs & Co., Principal Engineer, Hardware Engineering

Tom Garrison
Intel Corporation, Vice President & General Manager, Security Strategy and Initiatives, Client Computing Group

Baiju Patel, PhD
Intel Corporation, Intel Fellow – Security, Client Computing Group

Table of Contents

Summary

By the time a Personal Computer (PC) or a server (referred to as computing system in this document) is delivered to its intended customer, the sum of its parts has traveled through a highly complex supply chain. This supply chain includes diverse component suppliers, subsystem manufacturers, integrators, and original equipment manufacturers (referred to as suppliers in this document). The final product may go through several warehouses and may be transported via several shipping companies before it makes it to IT/end customer.

Considering ever-increasing threats to supply chain, customers have a growing need to know that the final product they received is indeed the product they ordered. Unintentional mistakes/errors, poor handling, or intentional fraud are key risks to the customer not receiving the system they ordered. Additional risks may come from malicious actors, including nation states and well-funded criminal organizations, who are motivated to tamper with systems in the supply chain. The consequences of these risks could include financial or reputational loss to the customer.

While many customers today treat a PC or Computing System as a "Black Box" and trust the supplier and transport, a growing portion of customers – such as Financial or Government Institutions – have additional procurement requirements. They are actively taking steps to ensure that the computing system, as delivered, meets their risk profile and can fulfill their compliance, security, and performance requirements.

Typically, these customers specify their requirements as part of their Request for Quotation (RFQ) process. The systems delivered to them are often evaluated by an in-house team or an external partner to ensure that the systems meet the requirements specified in the RFQ. However, it is only practical to evaluate a small subset of systems and results may not be available right away. This can either delay the deployment of systems or increase the risk by deploying a large number of systems before receiving all the results.

Source: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/next-security-frontier-intel-and-goldman-sachs.pdf

Preventing Counterfeit Components within your Manufacturing Supply Chain

Goal: Verify genuine device hardware & software configs upon receipt of manufactured devices and/or platforms

- Enables component-level traceability
- Mitigates risk of counterfeit electronic parts
- Facilitates compliance

Provide executive staff, auditors, partners, and/or customers with detailed reports on:

- Downstream Manufacturers
- Part Numbers
- Batch Numbers
- Distributors

Auto Verify Tools: Used by premier suppliers to identify system changes from the time of manufacturing to the time of first boot

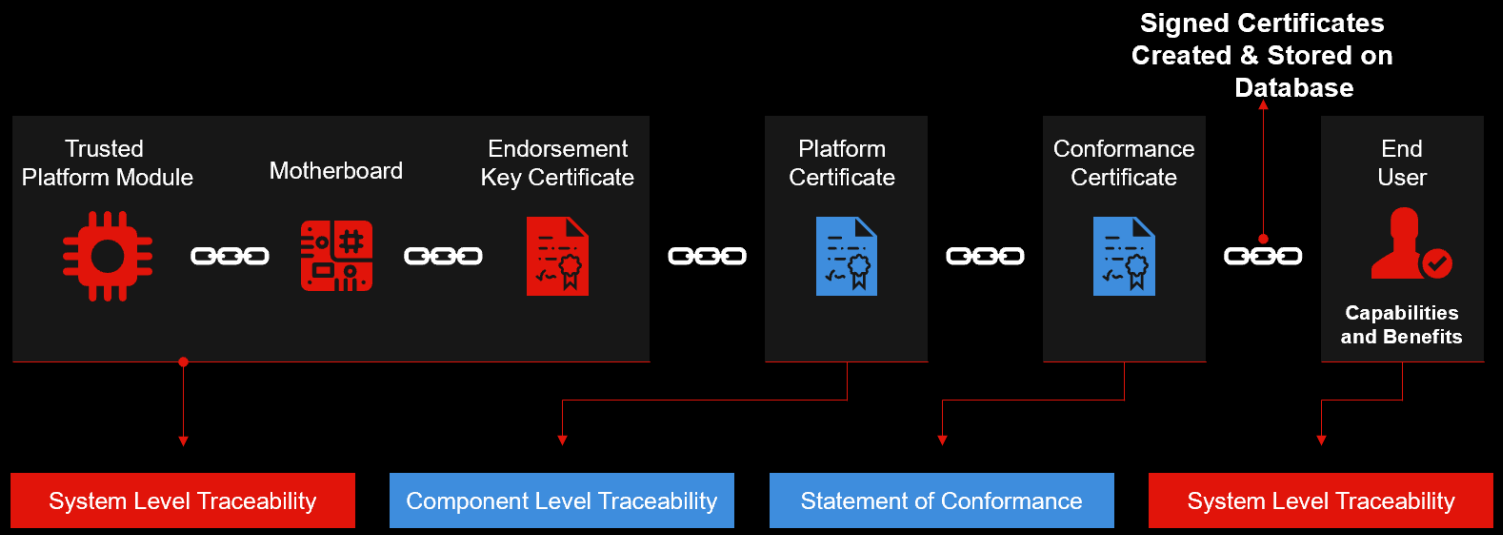
Preventing Counterfeit Components within your Manufacturing Supply Chain (Continued)

System Level Traceability: Signed platform certificates linked to discrete TPM on motherboard

Component Level Traceability: "As Built" report signed by manufacturer

Statement of Conformance: Attests to authenticity of system, signed by manufacturer

System Level Traceability: Customer access to signed files verifying integrity



How Cyber Attacks Directed Against Logistics & Fuel Suppliers Can Massively Disrupt Your Operations

- **Maersk Integrated Container Logistics & Supply Chain Services:**
  - 2017: NotPetya Cyber Attack
- **FedEx Transport Company**
  - 2017: NotPetya Cyber Attack
- **Colonial Pipeline**
  - 2021: Ransomware (“Darkside” Content Delivery Network [CDN]) Cyber Attack

Summary & Questions

Increasingly, large enterprise customers are requiring Original Design Manufacturers (ODMs) and/or Original Equipment Manufacturers (OEM) to show demonstrable proof that they have a secure supply chain. These manufacturers must prove, through controlled, documented, and audited means, that their supply chain ecosystem is secure throughout the product development lifecycle (pre-manufacturing through product end-of-life.)

This legitimate concern is based on the growing threat posed by second hand or counterfeit computing device components.

Disruptions in supply chains and the possible introduction of counterfeit components can increase risks to the proper functioning and overall reliability of electronic devices. Even worse, such contaminated platforms may include malware that could potentially lead to data theft or other types of system compromise.

To prevent this, organizations should only partner with technology vendors that provide verifiable proof that their products are free of second hand or counterfeit components.

To do so, a manufacturer should be able to trace serial numbers or similar identifiers that are stamped or embedded on hardware during downstream manufacturing. For software components, these manufacturers should work with their software vendors to ensure that only accurate, non-counterfeit software is ever installed on their products.

Kevin McPeak CISSP ITILv3
@kevin_mcpeak
linkedin.com/in/kevinmcpeak

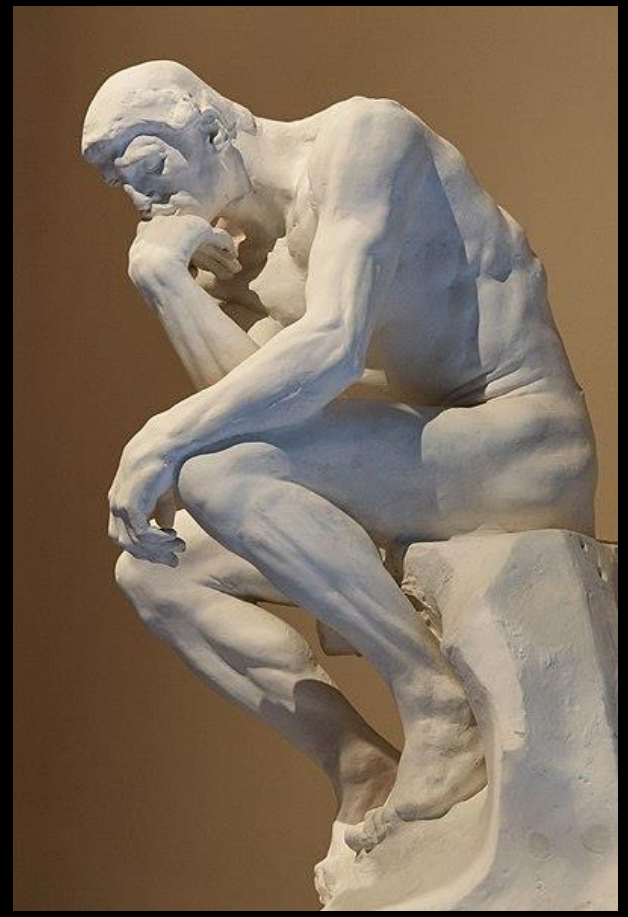


Image source: https://commons.wikimedia.org/wiki/File:The_Thinker_by_Auguste_Rodin,_Grand_Palais,_Paris_13_July_2017.jpg

Back-Up Slides:

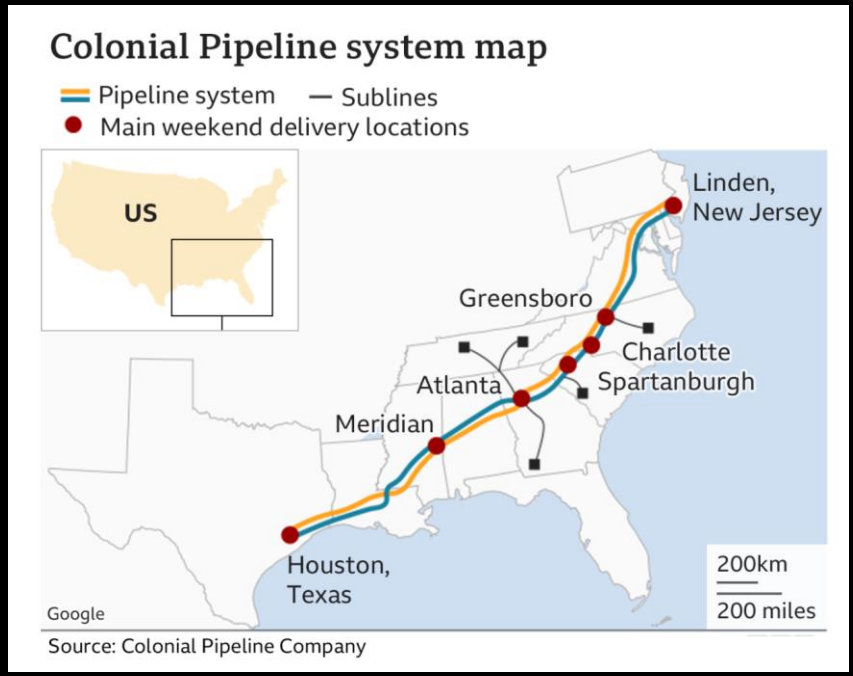
Technical Overview of the Cyber-Attack on the Colonial Pipeline

Kevin McPeak CISSP ITILv3
@kevin_mcpeak
linkedin.com/in/kevinmcpeak

ISSA Information Systems Security Association
Central Maryland Chapter

Colonial Pipeline:

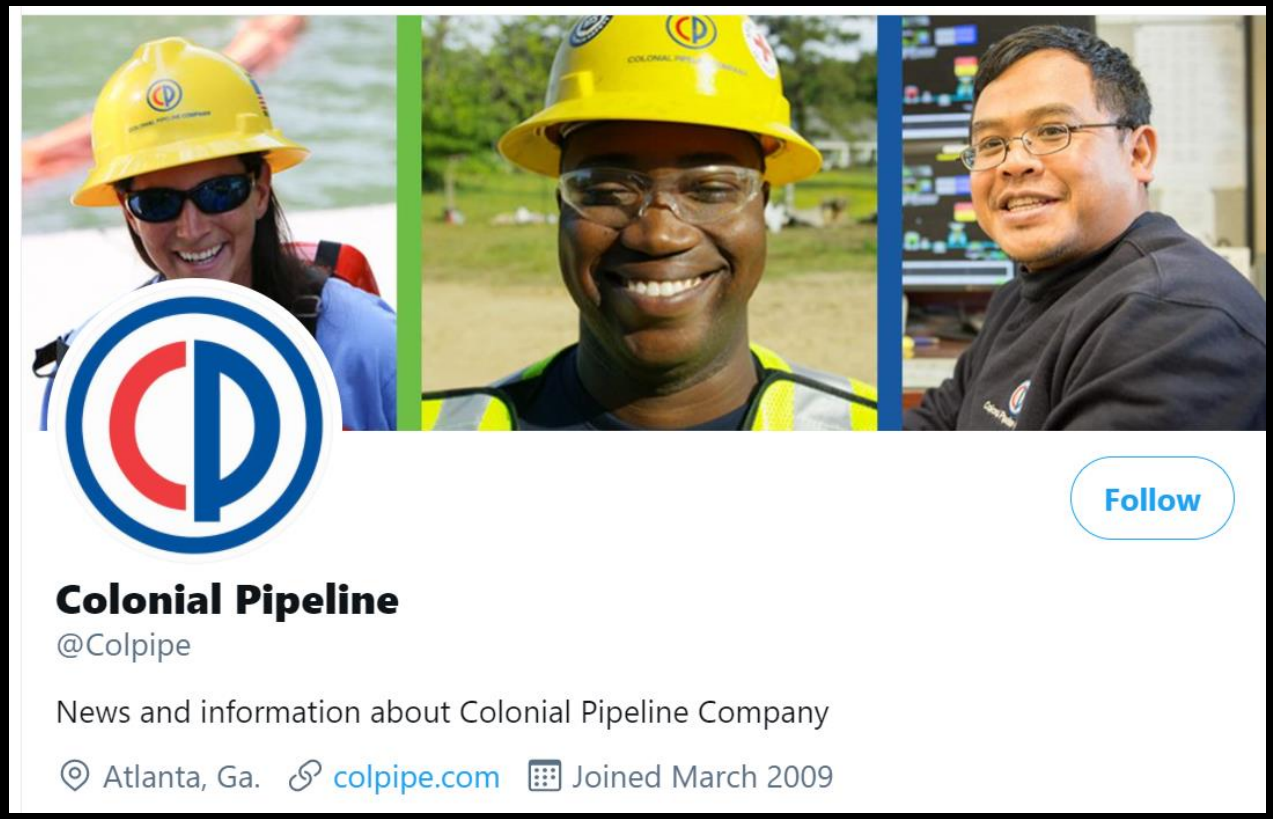
A Ransomware Attack that Led to Massive, Cascading, International Supply Chain Disruptions



Colonial Pipeline Cyber Attack

The Colonial Pipeline is:

- the largest pipeline system for refined oil products in the U.S.
- 5,500 miles (8,850 km) long
- capable of carrying 3 million barrels of fuel per day between Texas and New York.
- operated by Colonial Pipeline Company, which is headquartered in Alpharetta, GA

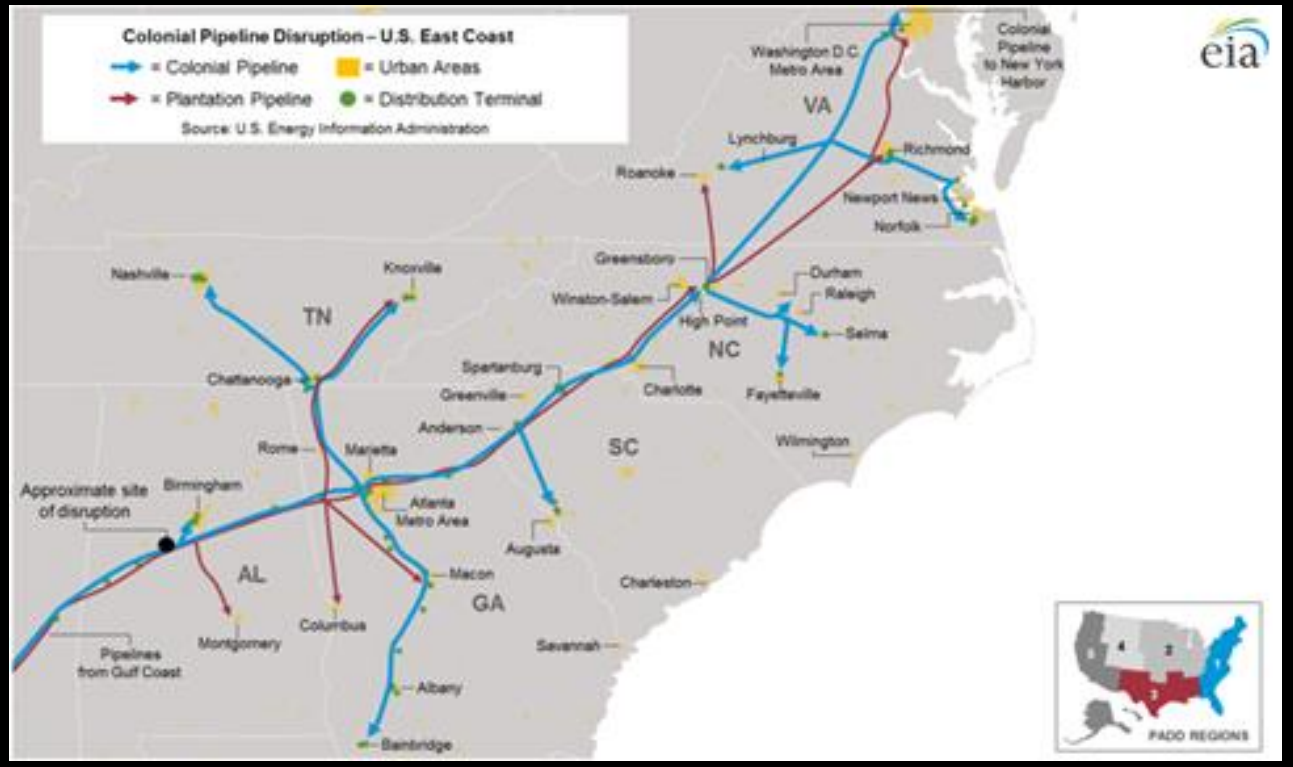


In the wake of September 11, Colonial Pipeline increased security at each of its facilities and created a comprehensive security plan. This was later recognized by the Federal Government as a model for the pipeline industry.

Colonial Pipeline Cyber Attack

Colonial Pipeline:

- Founded in 1961 and construction of the pipeline began in 1962.
- Consists of more than 5,500 mi (8,900 km) of pipeline, originating at Houston & terminating at the Port of NY & NJ.
- The pipeline travels through the coastal states of TX, LA, MS, AL, GA, SC, NC, VA, MD, DE, PA, & NJ.
- Branches from the main pipeline also reach TN.



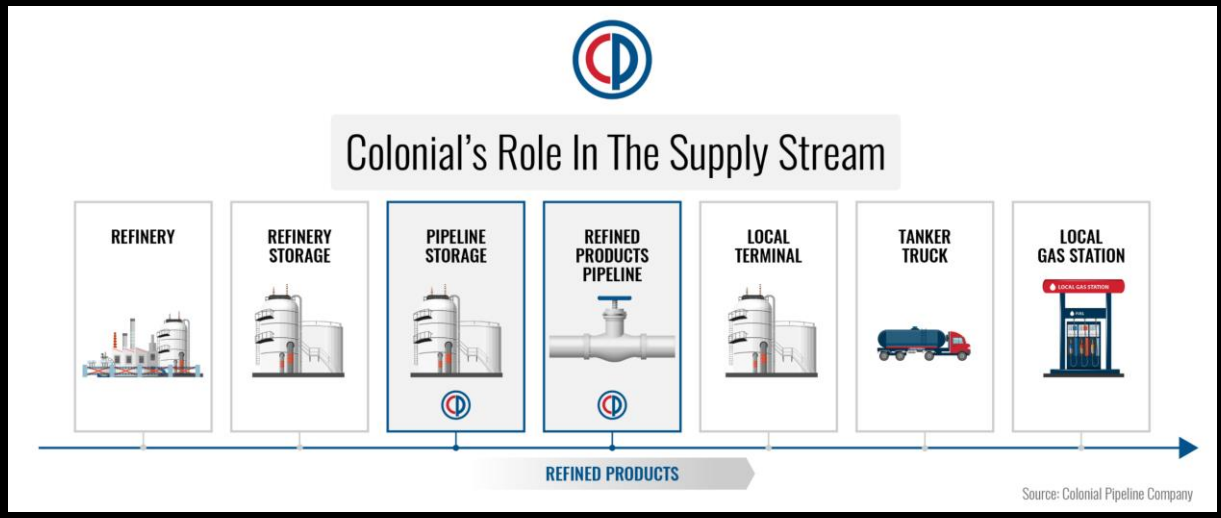
- The pipeline delivers a daily average of 100×106 (100,000,000) US gallons (3.8×108 L) of gasoline, home heating oil, aviation fuel & other refined petroleum products to communities & businesses throughout the South and Eastern United States.

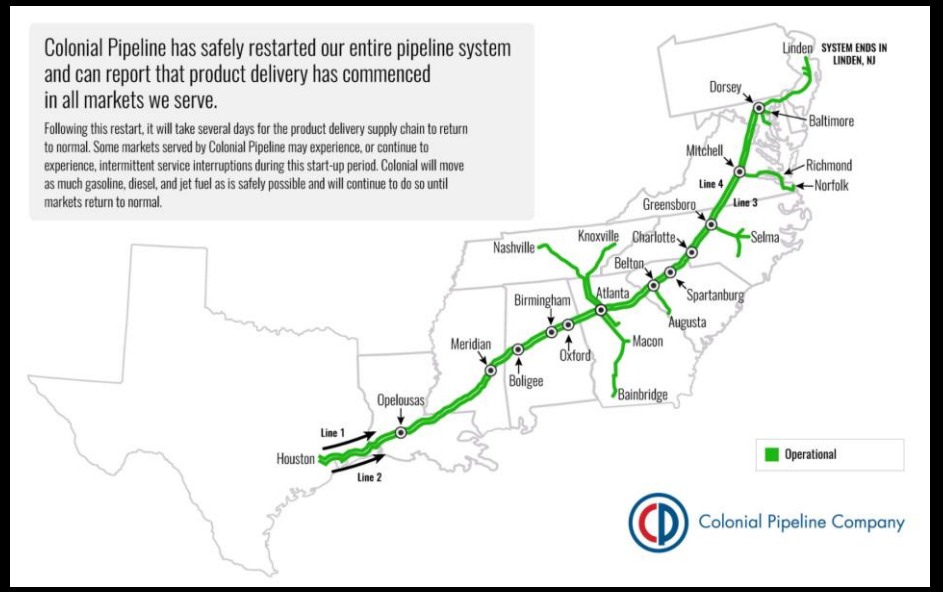
Image source: Energy Information Administration - Colonial Pipeline Disruption U.S. East Coast, Public Domain, https://commons.wikimedia.org/w/index.php?curid=85282933

Colonial Pipeline Cyber Attack

Colonial Pipeline:

- The main lines are 40 inches & 36 inches in (inner) diameter, with one primarily devoted to gasoline and the other carrying distillate products such as jet fuel, diesel fuel, and home heating oil.
- The pipeline connects directly to major airports along the system.
- 15 associated tank farms store more than 1.2×109 US gallons of fuel and provide a 45-day supply for local communities.
- Products move through the main lines at a rate of about 3 to 5 miles per hour.





- It generally takes from 14 to 24 days for a batch to get from Houston to the New York harbor, with 18.5 days the average time.

Colonial Pipeline Cyber Attack

Colonial Pipeline Ownership:

- Koch Industries (a.k.a. Koch Capital Investments Company LLC, 28.09% stake ownership)
- South Korea's National Pension Service and Kohlberg Kravis Roberts (a.k.a. Keats Pipeline Investors LP, 23.44% stake ownership)
- Caisse de dépôt et placement du Québec (16.55% stake ownership via CDPQ Colonial Partners LP, acquired in 2011)
- Royal Dutch Shell (a.k.a. Shell Pipeline Company LP, 16.12% stake ownership)
- IFM Investors (a.k.a. IFM (US) Colonial Pipeline 2 LLC, 15.80% stake ownership, acquired in 2007)

Colonial Pipeline Cyber Attack

Colonial Pipeline Innovations:

- 1978 - Colonial Pipeline became the first company to equip gasoline storage tanks with geodesic domes.
- 1985 - Colonial Pipeline began use of caliper and magnetic pigs to detect anomalies in the lines.
- 1994 - following a historic flood that ruptured a number of pipelines at the San Jacinto River near Houston, Colonial Pipeline directionally drilled 30 feet beneath the river and floodplain to install two new 3,100-foot permanent pipelines.

Image source: https://upload.wikimedia.org/wikipedia/commons/f/f9/Hart_visits_Colonial_Pipeline_Dorsey_Junction_Facility.jpg
Attribution: National Transportation Safety Board, Public domain, via Wikimedia Commons]

Colonial Pipeline Cyber Attack

Colonial Pipeline 2021: May 7 Malware Attack

- The attack focused on Colonial Pipeline's payment system – therefore, the pipeline was proactively shut down on May 9.
- Approximately 12,000 gas stations were directly affected by the shutdown.
- Operations were restored on May 13.
- The shutdown led to temporary fuel shortages along the East Coast.

Colonial Pipeline attack: Everything you need to know

Updated: DarkSide has claimed responsibility for the catastrophic ransomware outbreak.

By Charlie Osborne for Zero Day | May 13, 2021 -- 07:17 GMT (00:17 PDT) | Topic: Security

The real-world consequences of a successful cyberattack have been clearly highlighted this week with the closure of one of the US' largest pipelines due to ransomware.

Here's everything we know so far.

On Friday, May 7, Colonial Pipeline said that a cyberattack forced the company to proactively close down operations and freeze IT systems after becoming the victim of a cyberattack.

This measure "temporarily halted all pipeline operations" and cybersecurity firm FireEye, which operates the Mandiant cyberforensics team, was reportedly pulled in to assist.

ZDNET RECOMMENDS

Best VPN services

Best security keys

Best antivirus software

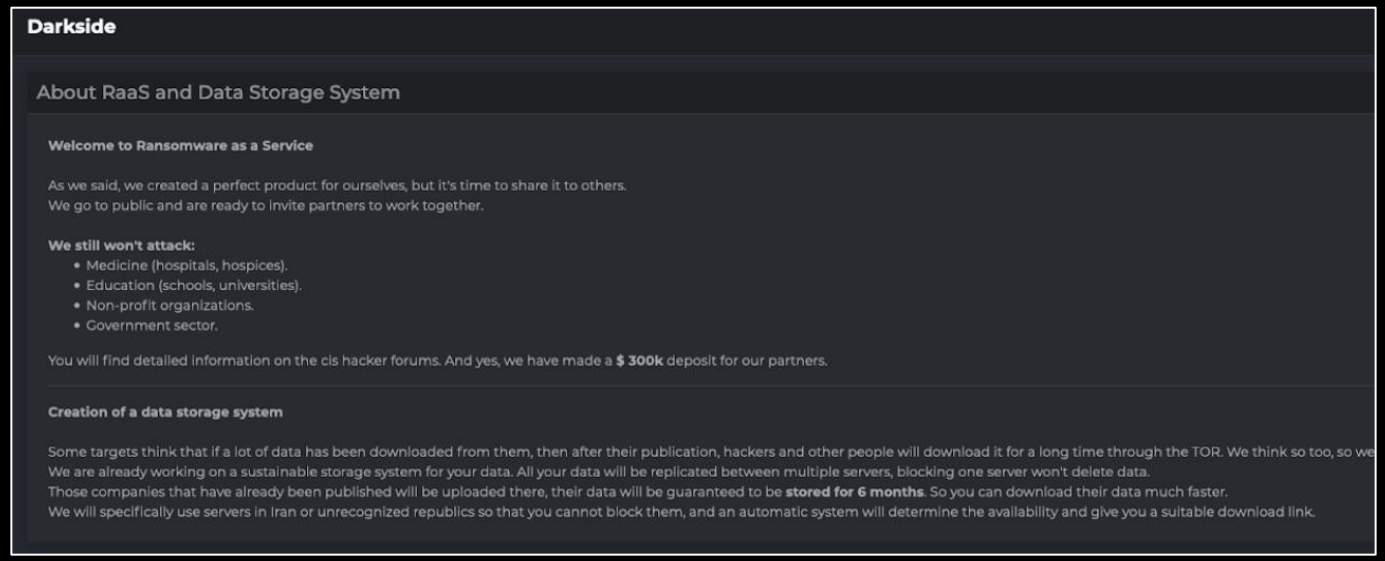
The fastest VPNs

- The attack on the Colonial Pipeline has been attributed to "DarkSide," a relatively new (at that time) ransomware family that emerged on the crimeware market in November 2020.

Colonial Pipeline Cyber Attack

DarkSide:

- DarkSide launched as a RaaS (Ransomware-as-a-Service)
- Stated goal of only targeting ‘large corporations’
- Primarily focused on recruiting Russian (CIS) affiliates
- Very skeptical of partnerships or interactions outside of that region
- From the onset, DarkSide was focused on choosing the ‘right’ targets and identifying their most valuable data. This speaks to their efficiency and discernment when choosing where to focus their efforts.
- DarkSide claims to not attack medical, educational, non-profit, or government sectors.

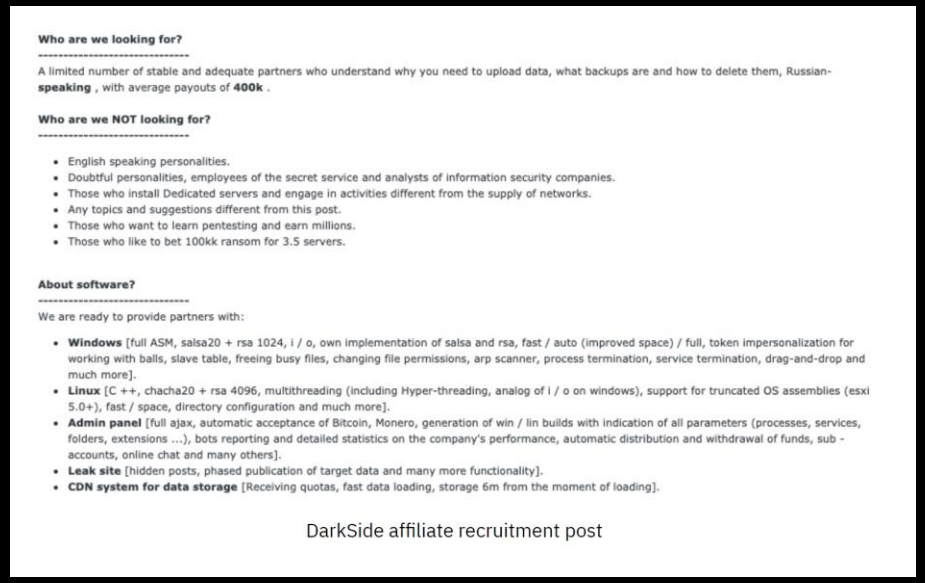


Source: https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/

Colonial Pipeline Cyber Attack

DarkSide:

- At the time of launch, the features offered by DarkSide were fairly standard.
- They emphasized their speed of encryption & a wealth of options for dealing with anything that may inhibit the encryption process (i.e., security software).
- They also advertised a Linux variant with comparable features.
- Following in the footsteps of recently successful ransomware families like Maze and Cl0p, DarkSide established a victim data leaks blog as further leverage to encourage ransom payouts.



Who are we looking for?

A limited number of stable and adequate partners who understand why you need to upload data, what backups are and how to delete them, Russian-**speaking** , with average payouts of **400k** .

Who are we NOT looking for?

- English speaking personalities.
- Doubtful personalities, employees of the secret service and analysts of information security companies.
- Those who install Dedicated servers and engage in activities different from the supply of networks.
- Any topics and suggestions different from this post.
- Those who want to learn pentesting and earn millions.
- Those who like to bet 100kk ransom for 3.5 servers.

About software?

We are ready to provide partners with:

- **Windows** [full ASM, salsa20 + rsa 1024, i / o, own implementation of salsa and rsa, fast / auto (improved space) / full, token impersonalization for working with balls, slave table, freeing busy files, changing file permissions, arp scanner, process termination, service termination, drag-and-drop and much more].
- **Linux** [C ++, chacha20 + rsa 4096, multithreading (including Hyper-threading, analog of i / o on windows), support for truncated OS assemblies (esxi 5.0+), fast / space, directory configuration and much more].
- **Admin panel** [full ajax, automatic acceptance of Bitcoin, Monero, generation of win / lin builds with indication of all parameters (processes, services, folders, extensions ...), bots reporting and detailed statistics on the company's performance, automatic distribution and withdrawal of funds, sub - accounts, online chat and many others].
- **Leak site** [hidden posts, phased publication of target data and many more functionality].
- **CDN system for data storage** [Receiving quotas, fast data loading, storage 6m from the moment of loading].

DarkSide affiliate recruitment post

The original DarkSide 1.0 Feature set was advertised as follows:

```
Windows [
        full ASM, salsa20 + rsa 1024,
        i / o, own implementation of salsa and rsa,
        fast / auto (improved space) / full,
        token impersonalization for working with balls,
        slave table, freeing busy files,
        changing file permissions,
        arp scanner,
        process termination,
        service termination,
        drag-and-drop and much more].

Linux [
        C ++, chacha20 + rsa 4096,
        multithreading (including Hyper-threading, analog of i / o on windo
        support for truncated OS assemblies (esxi 5.0+),
        fast / space,
        directory configuration and much more].

Admin panel [
        full ajax,
        automatic acceptance of Bitcoin, Monero,
        generation of win / lin builds with indication of all parameters (
        bots reporting and detailed statistics on the company's performanc
        automatic distribution and withdrawal of funds,
        sub -accounts,
        online chat and many others].

Leak site [
        hidden posts,
        phased publication of target data and many more functionality].

CDN system for data storage [
        Receiving quotas,
        fast data loading,
        storage 6m from the moment of loading].
```

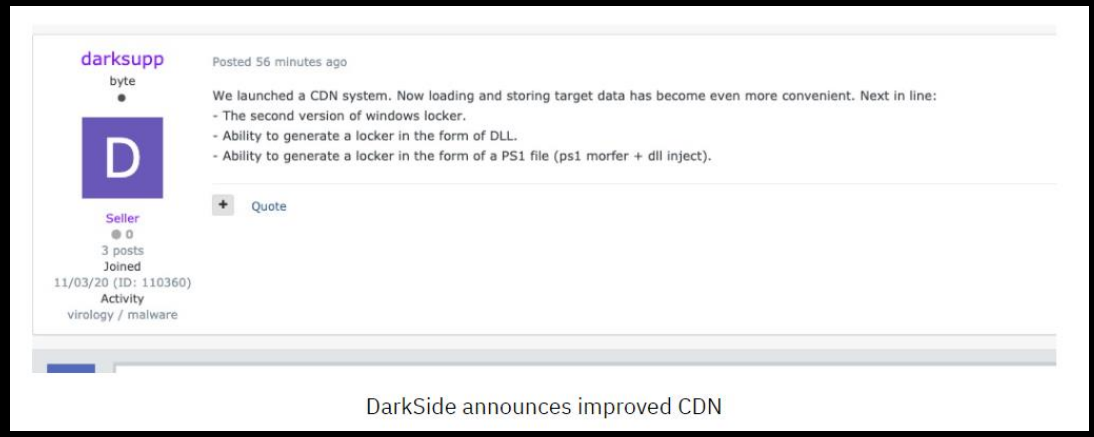
A Well-Organized Affiliate Network:
Hopeful affiliates are subject to DarkSide's rigorous vetting process, which examines the candidate's 'work history,' areas of expertise, and past profits among other things. To get started, affiliates were required to deposit 20 BTC (at the time, that amounted to around $300,000 USD).

Source: https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/

Colonial Pipeline Cyber Attack

DarkSide CDN:

- Over the following months, DarkSide continued to improve its services, while also expanding its affiliate network.
- By late November 2020, DarkSide launched a more advanced Content Delivery Network (CDN) that allowed their operators to more efficiently store and distribute stolen victim data.
- Many of their high-value targets found themselves listed on the victim blog, including a number of financial, accounting, and legal firms, as well as technology companies.
- Initial access can take many forms depending on the affiliate involved, their needs, and timeline.
- A majority of the campaigns observed were initiated only after the enterprise had been thoroughly scouted via Cobalt Strike beacon infections.
- After the initial reconnaissance phase, the operators would deploy the DarkSide ransomware wherever it would cause the greatest disruption.



DarkSide announces improved CDN

Source: https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/

Colonial Pipeline Cyber Attack

DarkSide 2.0 Technical Capabilities:

By March, DarkSide announced the launch of the new & improved DarkSide 2.0. The new iteration included many improvements for Windows and Linux variants & was no longer subject to a decryption tool that had been developed by Bitdefender. DarkSide 2.0 reportedly encrypts data on disk twice as fast as the original.

Other updated features included:

- Expanded multi-processor support (parallel/simultaneous encryption across volumes)
- EXE and DLL-based payloads
- Updated SALSA20+RSA1024 implementation with “proprietary acceleration”
- New operating modes (Fast / Full / Auto)
- 19 total build settings
- Active account impersonation
- Active Directory support (discovery and traversal)
- New CMD-line parameter support

On the Linux side, DarkSide 2.0 offered the following updates:

- Updated multithreading support
- Updated CHACHA20 + RSA 4096 implementation

2 new operating modes (Fast / Space)

14 Total build settings

Support for all major ESXi versions

NAS support (Synology, OMV)

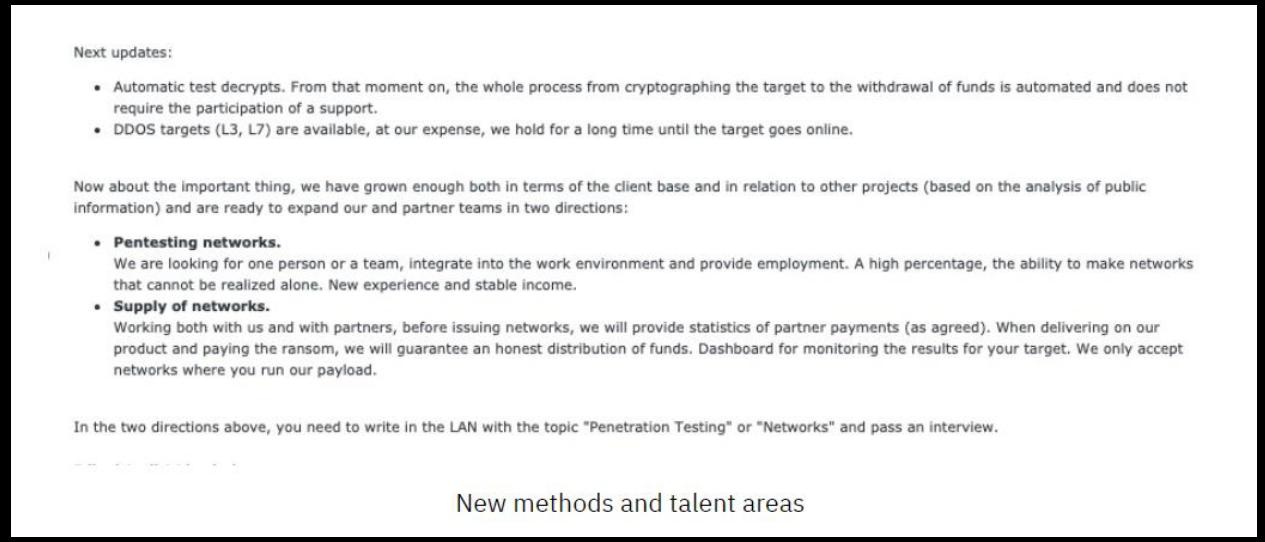
Along with this expanded feature set, researchers have seen a shift in the deployment of the DarkSide ransomware, from standard packers like VMProtect and UPX to a custom packer internally referred to as ‘encryptor2.’

Source: https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/

Colonial Pipeline Cyber Attack

DarkSide – A Growing Threat:

- With the release of DarkSide 2.0, the group has continued to increase its footprint in the Ransomware landscape.
- Along with their territorial expansion throughout 2021, DarkSide also increased their ‘pressure campaigns’ on victims to include DDoS attacks along with the threat of data leakage.
- DarkSide is able to invoke L3/L7 DDoS attacks if their victims choose to resist ‘cooperation.’
- More recently, DarkSide operators have been attempting to attract more expertise around assessing data and network value, along with seeking others to provide existing access or newer methods of initial access.
- These efforts are meant to make operations more streamlined and increase efficiency.



Next updates:

- Automatic test decrypts. From that moment on, the whole process from cryptographing the target to the withdrawal of funds is automated and does not require the participation of a support.
- DDOS targets (L3, L7) are available, at our expense, we hold for a long time until the target goes online.

Now about the important thing, we have grown enough both in terms of the client base and in relation to other projects (based on the analysis of public information) and are ready to expand our and partner teams in two directions:

- **Pentesting networks.**
  We are looking for one person or a team, integrate into the work environment and provide employment. A high percentage, the ability to make networks that cannot be realized alone. New experience and stable income.
- **Supply of networks.**
  Working both with us and with partners, before issuing networks, we will provide statistics of partner payments (as agreed). When delivering on our product and paying the ransom, we will guarantee an honest distribution of funds. Dashboard for monitoring the results for your target. We only accept networks where you run our payload.

In the two directions above, you need to write in the LAN with the topic "Penetration Testing" or "Networks" and pass an interview.

New methods and talent areas

Source: https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/

Colonial Pipeline Cyber Attack

Lessons Learned:

- The Colonial Pipeline attack is only the latest in a slew of increasingly daring ransomware attacks. DHS Secretary Alejandro Mayorkas stated that ransomware attacks cost victims a combined $350 million in 2020.
- The absolute best defense against a severe ransomware attack (and the nightmare that follows) is preparation and prevention.
- Technology is a huge part of that, but one must not discount user hygiene and education.
- It is vital to keep end users up to date on what threats are out there and how to spot them.
- Vigilant users, along with robust preventative controls are key.
- Business continuity planning and disaster recovery drills are not fun, but they are critical and necessary to ensure readiness and resilience against these threats.

MITRE ATT&CK

T1112 Modify Registry

T1012 Query Registry

T1082 System Information Discovery

T1120 Peripheral Device Discovery

T1005 Data from Local System

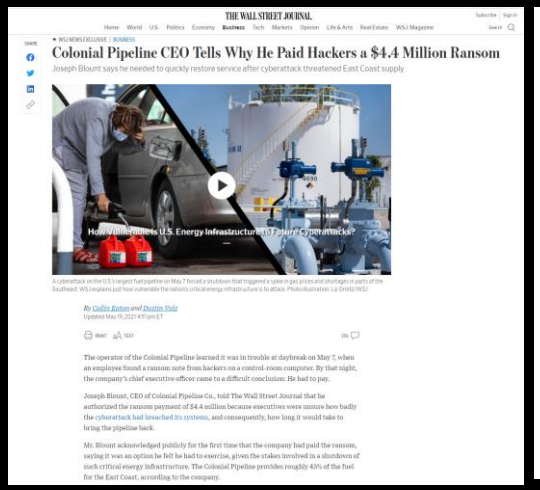
T1486 Data Encrypted for Impact

T1543.003 Create or Modify System Process: Windows Service

T1490 Inhibit System Recovery

T1553.004 Subvert Trust Controls: Install Root Certificate

T1078 Valid Accounts


THE WALL STREET JOURNAL.

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supply


Owners of Colonial Pipeline Hit With Class Action Regarding Allegedly Deficient Cybersecurity Following Hack, Showing All Data Breaches Carry Litigation Risk

By Kristin Bryan, Ericka Johnson and Sarah Rathke on May 20, 2021

POSTED IN SUPPLY CHAIN

This is a Cross-Post from Consumer Privacy World. Please contact Kristin Bryan with any questions.

Well, that took no time at all. On May 19, 2021, the first class action was filed against the owners of the Colonial Pipeline by a putative class of customers, based on alleged elevated fuel prices as a result of the cyberattack. Consumers are obviously the endpoint of this and almost any supply chain, but there are bound to be B2B lawsuits as well, by entities at both ends of this critical supply chain point. We'll be tracking these, so stay tuned!

Sources: https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/
https://www.mondaq.com/unitedstates/trials-appeals-compensation/1072236/owners-of-colonial-pipeline-hit-with-class-action-regarding-allegedly-deficient-cybersecurity-following-hack-showing-all-data-breaches-carry-litigation-risk
https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636