RANSOMWARE THREATS & TRENDS

June 30, 2021

accenturesecurity

LEGAL NOTICE & DISCLAIMER: © 2021 Accenture. All rights reserved. Accenture, the Accenture logo, Accenture CTI and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture CTI. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change.
ACCENTURE PROVIDES THE INFORMATION ON AN "AS-IS" BASIS WITHOUT REPRESENTATION OR WARRANTY AND ACCEPTS NO LIABILITY FOR ANY ACTION OR FAILURE TO ACT TAKEN IN RESPONSE TO THE INFORMATION CONTAINED OR REFERENCED IN THIS ALERT.

This report is classified TLP:AMBER (https://first.org/tlp/). Information contained within this report may not be shared beyond the recipient's organization and is subject to the confidentiality clauses between the recipient and Accenture.

Agenda

Global cybersecurity events are having a massive impact on how organizations address security and resilience

1. Energy Cyber Threat Landscape
2. Executive Order Overview
3. Colonial Pipeline Ransomware Event
4. TSA Pipeline Directive

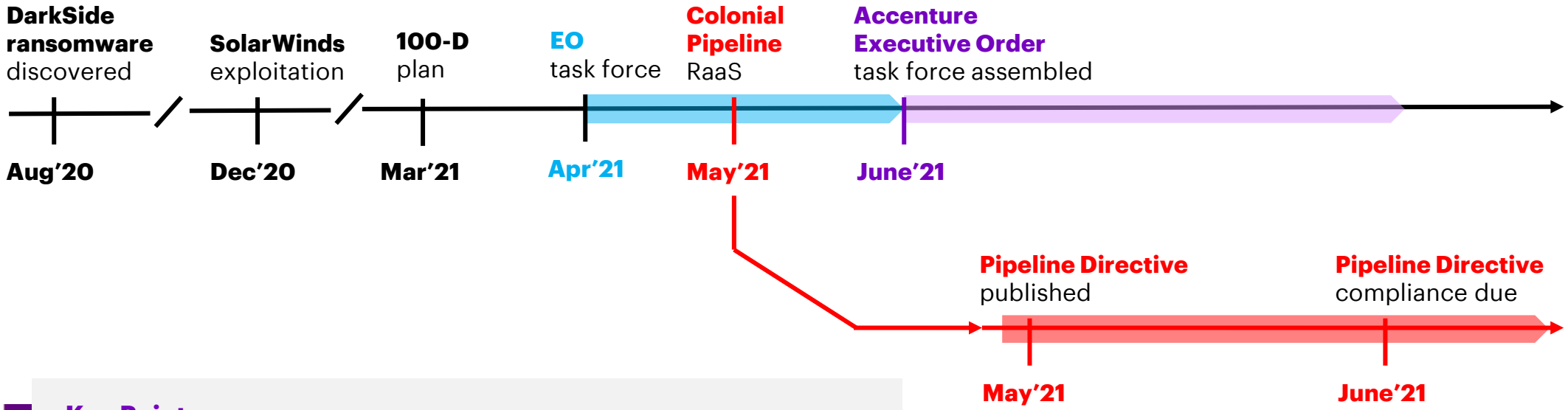
Copyright © 2021 Accenture. All rights reserved.

Energy Cyber Threat Landscape

Copyright © 2021 Accenture. All rights reserved.

2020-2021 Chain of Events

Briefing overview



Key Points

The Executive Order The EO started in the early days of the current administration, along with the 100-day plan for Utilities

Darkside attribution Earliest indication of DarkSide providing ransomware as a service (RaaS) was in the summer of 2020

Dramatic increase in RaaS There has been a significant increase in overall ransomware attacks from 2020 to 2021

100-Day Plan Current administration has identified 6 major utilities who provide power to a list of USG critical sites that must have specific threat anomaly detection included *(Timeframe 4/16/2021-7/25/2021)*

Copyright © 2021 Accenture. All rights reserved.

Ransomware Attack Threats & Trends

Remote Work
- During COVID-19, many companies switched to WFH policies, which made RDP and VPN highly targeted

Delay in Patching
- Threat actors target 1-day vulns

Third-parties
- Threat actors utilize third-parties/supply chain companies, as a means to reach victims with larger revenue

Ransomware gang business models streamline attack methods
- Affiliate programs
- Streamlined attacks
- No attribution
- Mis-attribution
- Nation-state threat actors absolved from blow-back

NetWalker
- Various energy sector victims

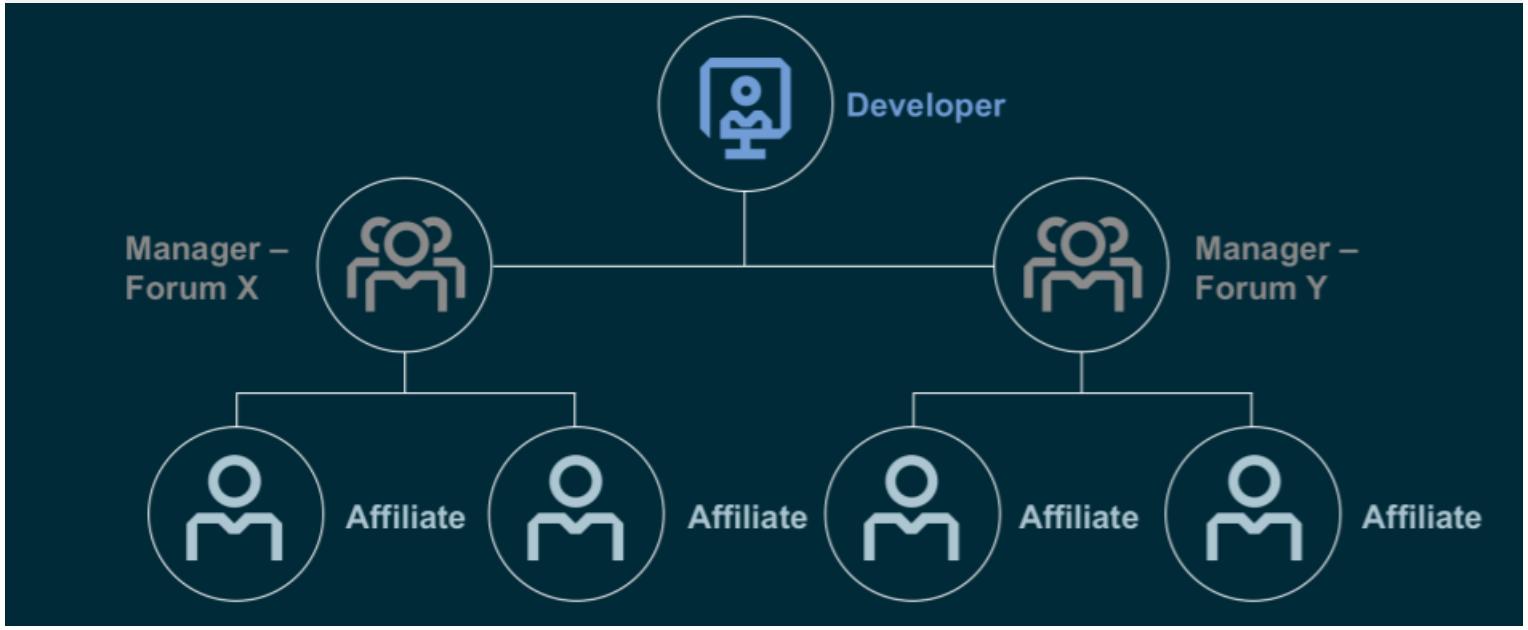
CLOP
- Linked to Accellion File Transfer Alliance (FTA) exploit, according to Bleeping Computer

Darkside
- Linked to Colonial Pipeline ransomware event, according to FBI

Copyright © 2021 Accenture. All rights reserved.

Ransomware affiliate business model

Ransomware Business Model: **Affiliate**



An “affiliate” program may be managed by the malware author(s) themselves or an individual that has purchased the ransomware with distribution rights.

Copyright © 2021 Accenture. All rights reserved.

The Executive Order

"[...W]e cannot fight the threat posed by ransomware alone. The private sector has a distinct and key responsibility. The federal government stands ready to help you implement these best practices."

Anne Neuberger, White House Deputy National Security Adviser
for Cyber and Emerging Technology
Wall Street Journal

Copyright © 2021 Accenture. All rights reserved.

Executive summary

Background

- A draft executive order on cybersecurity is being finalized by the White House. An **April 2021 release.**
- The order was spurred by the SolarWinds cyberattack, which involved a software breach impacting roughly 100 private sector companies and nine U.S. Federal Agencies, including NASA.
- At a US Senate Intelligence hearing, executives from SolarWinds, Microsoft, FireEye, and CrowdStrike called for **greater transparency and information-sharing of cyberattacks and breaches.**
- The order proposes significant policy changes, empowering the government to:
  - Adapt to the changing environment, particularly around detection and response.
  - Ensure that products are securely built and that supply chains are secured.
  - Build collaborations with the commercial sector (public, private partnership).
- **All software and SaaS contractors doing business with the US government will have to meet new software security standards** and swiftly report cyber incidents to a new, as yet undefined entity within the Department of Homeland Security.
- **Specific requirements will be developed by NIST** and are expected to be effective in the next several months, after a public comment period.

Highlights

- **Significant increases in authority and resources for the government** to run/coordinate/standardize the security of civilian federal networks (e.g., incident response playbooks, endpoint detection and response, logging event data).
- Creates **mandatory incident reporting** to the federal government for every software and SaaS provider.
- Federal and Defense contracts with providers shall contain **no barriers to sharing of data** related to event prevention, detection and response.
- Software suppliers will need to **attest to the security of their software development lifecycle.**
- Directs a swift increase in the pace of federal government agencies to **transition to the cloud and adopt a zero-trust model.**

Copyright © 2021 Accenture. All rights reserved.

Colonial Pipeline Ransomware Event

"A May 7 ransomware attack on Colonial Pipeline Co. led to a six-day shutdown of the East Coast's largest conduit for fuel, sparking scrutiny of pipeline security and pushing the Department of Homeland Security to prepare to issue first-of-their-kind cybersecurity regulations for the sector."

Wall Street Journal

Copyright © 2021 Accenture. All rights reserved.

Colonial Pipeline ransomware event

- May 7th Colonial Pipeline shut down due to a ransomware attack reportedly **impacting only their IT Systems**. Flow of 2.5 Million Gallons of fuel per day disrupted.
- Motivation **appears to be financial with no broader energy industry campaign**. No indication of strategic Russian state interests.
- FBI has confirmed the involvement of "**DarkSide Ransomware**." Darkside is a **Ransomware as a Service (RaaS)** operator who has since "retired". Emerged in mid-2020 and only targets organizations that have the financial **resources to pay large ransoms**.

Copyright © 2021 Accenture. All rights reserved.

The Pipeline Directive

"A May 7 ransomware attack on Colonial Pipeline Co. led to a six-day shutdown of the East Coast's largest conduit for fuel, sparking scrutiny of pipeline security and pushing the Department of Homeland Security to prepare to issue first-of-their-kind cybersecurity regulations for the sector."

Wall Street Journal

Copyright © 2021 Accenture. All rights reserved.

TSA directive

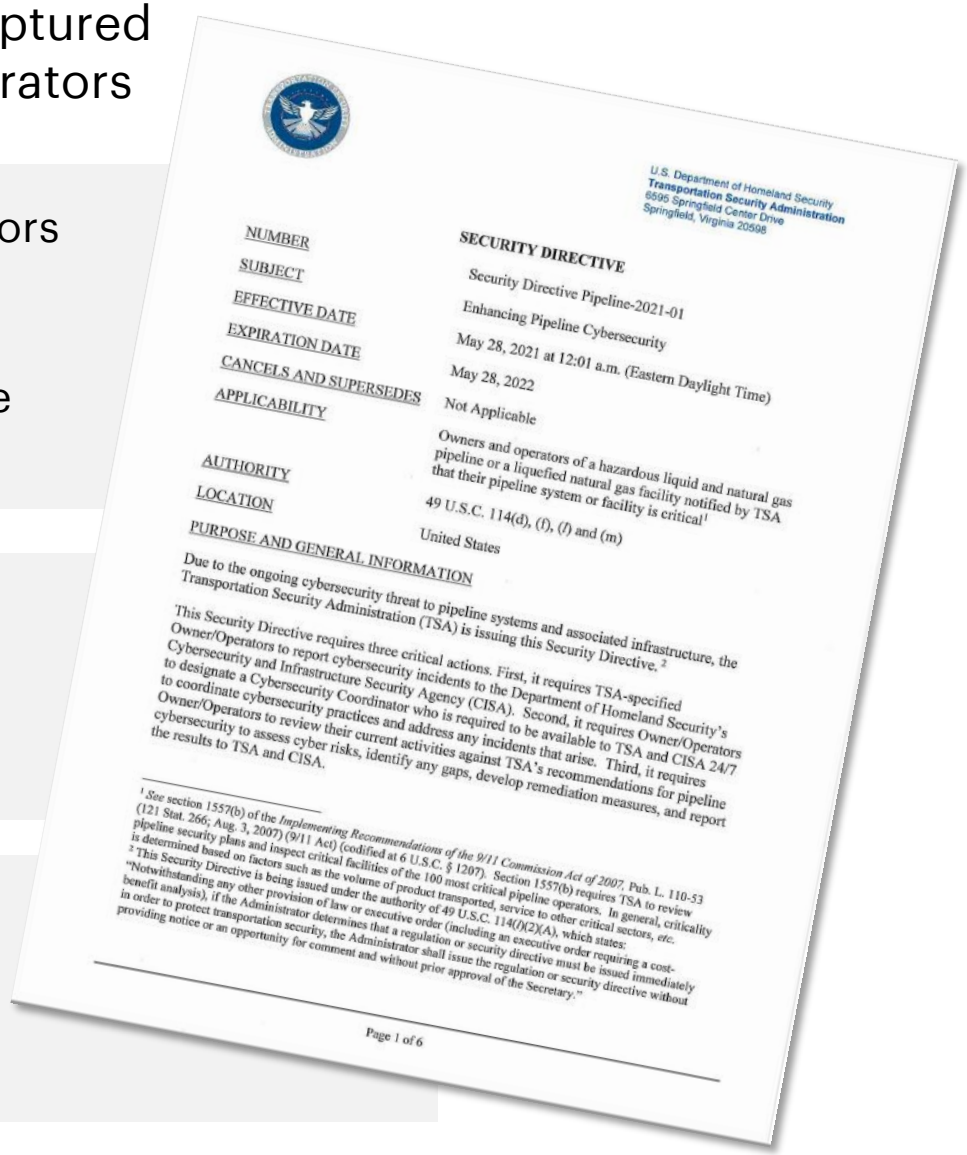
As per TSA directive dated 05/27, three key elements are captured highlighting key call for actions for pipeline owners and operators

As per TSA require critical pipeline owners and operators to report confirmed and potential cybersecurity incidents to the CISA

Designate a Cybersecurity Coordinator, to be available 24 hours a day, seven days a week

Pipeline owners and operators to review their current practices to identify any gaps and related remediation measures

Perform cyber-related risks and report the results to TSA and CISA within 30 days; due to TSA June 25th



U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

SECURITY DIRECTIVE

NUMBER	Security Directive Pipeline-2021-01
SUBJECT	Enhancing Pipeline Cybersecurity
EFFECTIVE DATE	May 28, 2021 at 12:01 a.m. (Eastern Daylight Time)
EXPIRATION DATE	May 28, 2022
CANCELS AND SUPERSEDES	Not Applicable
APPLICABILITY	Owners and operators of a hazardous liquid and natural gas pipeline or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical[1]
AUTHORITY	49 U.S.C. 114(d), (f), (*l*) and (m)
LOCATION	United States

PURPOSE AND GENERAL INFORMATION

Due to the ongoing cybersecurity threat to pipeline systems and associated infrastructure, the Transportation Security Administration (TSA) is issuing this Security Directive.[2]

This Security Directive requires three critical actions. First, it requires TSA-specified Owner/Operators to report cybersecurity incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Second, it requires Owner/Operators to designate a Cybersecurity Coordinator who is required to be available to TSA and CISA 24/7 to coordinate cybersecurity practices and address any incidents that arise. Third, it requires Owner/Operators to review their current activities against TSA's recommendations for pipeline cybersecurity to assess cyber risks, identify any gaps, develop remediation measures, and report the results to TSA and CISA.

[1] *See* section 1557(b) of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Pub. L. 110-53 (121 Stat. 266; Aug. 3, 2007) (9/11 Act) (codified at 6 U.S.C. § 1207). Section 1557(b) requires TSA to review pipeline security plans and inspect critical facilities of the 100 most critical pipeline operators. In general, criticality is determined based on factors such as the volume of product transported, service to other critical sectors, *etc.*

[2] This Security Directive is being issued under the authority of 49 U.S.C. 114(*l*)(2)(A), which states: "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary."

Page 1 of 6

Copyright © 2021 Accenture. All rights reserved.

Thank You