Tracking DarkSide and Ransomware: The Network View

By Joe Slowik

Published: 2021-05-17 · Archived: 2026-04-06 00:13:21 UTC

Updated October 14, 2021.

Since grabbing headlines in early May 2021, the ransomware incident impacting Colonial Pipeline attracted significant attention from both media and information security spaces, given the scope and impact of the event. While much has already been written and will continue to emerge as more evidence comes available, lacking from the discussion so far is a network-centric view of the general behaviors and detection possibilities associated with ransomware deployment. In this article, Gigamon provides an overview of the event in question, the behaviors linked to similar ransomware operations, the importance of network visibility, and possibilities for network detection and monitoring to meet these adversaries and related malicious activities head-on.

Background

On May 7, 2021, Colonial Pipeline suffered a ransomware incident. While all available information indicates that ransomware impacted only enterprise IT systems for Colonial, the company preemptively shut down linked industrial control systems (ICS) out of an abundance of caution. The intrusion and resulting disruption were subsequently linked to a ransomware variant known as DarkSide. Active since at least August 2020, DarkSide operates under a "Ransomware as a Service" or "affiliate" model where the group provides "double-extortion" ransomware services to other entities that execute the actual network breach and capability deployment. DarkSide then manages negotiations and payment to both decrypt a victim's information and to stop the selective leaking of data exfiltrated from the target network.

While DarkSide-related activity has continued at a relatively steady state since its initial discovery in 2020, the Colonial Pipeline incident is notable given its disruptive impact. While neither the first notable cyber intrusion in pipeline systems, nor the first ransomware event on pipeline infrastructure, Colonial's preemptive shutdown of critical systems triggered a halt in their operations. As one of the main arteries delivering refined petroleum products to the Eastern and Southeastern United States, the disruption induced reactions from panic buying of gasoline through statements from the White House. Although Colonial was able to begin restoring operations as early as May 12, 2021, the shock and short-term impacts of the event were felt across both policymaker and information security circles.

Ransomware Entity Intrusion Tradecraft

DarkSide ransomware impacted multiple victims since discovery in 2020. Yet while this ultimate payload inducing network disruption (and data theft for extortion) is concerning, defenders should focus on the preliminary steps enabling ransomware execution rather than the ransomware family itself. In this respect, given the "affiliate model" through which adversaries deploy DarkSide, the ransomware variant can be linked to multiple behavioral profiles.

Multiple vendors provide insight into initial access, entrenchment, and subsequent lateral movement activity linked to DarkSide deployment. Among the most notable examples are the following:

- Initial reporting from Digital Shadows in September 2020
- Cyberreason Nocturnus' overview of activity in April 2021
- Varonis reporting, subsequently updated after the Colonial incident
- An overview of recent DarkSide behaviors from FireEye, also after the Colonial incident
- Observations from incident response engagements from Sophos
- Further analysis from Palo Alto Unit 42

These are all valuable contributions to the discussion concerning DarkSide's deployment, and Gigamon highly recommends defenders review these items for awareness and to become familiar with this threat. Yet all these items largely focus on host-based actions and observations, which is unsurprising, as most of the entities in question are involved in host-based security solutions. In addition to these observations, defenders possess a multitude of options for tracking behaviors over the network related to DarkSide deployment, as well as other ransomware operations.

Initial Access Mechanisms

Adversary deployment of DarkSide ransomware is linked to a variety of initial access mechanisms, as one would expect given that multiple entities relate to its use. Based on a review of available literature and analysis, Gigamon identifies the following as primary Darkside affiliate mechanisms to initially breach victim networks:

- Phishing activity leveraging malicious attachments
- Credential replay attacks against external-facing services, such as Remote Desktop Protocol (RDP)
- Use of publicly disclosed exploits against external-facing services, such as vulnerabilities in externally accessible VPN appliances (including CVE-2021-20016)

While the above represent known vectors linked to DarkSide affiliate operations, the specific mechanism used to infiltrate Colonial Pipeline is not known at the time of this writing. Nonetheless, these initial intrusion mechanisms align well with common tradecraft associated with not only criminal operations (such as ransomware), but also advanced persistent threat (APT) or state-directed intrusions.

While one specific VPN exploit is called out in research from FireEye, Gigamon assesses that other, publicly disclosed exploits have also likely been used as part of intrusions leading to ultimate ransomware deployment more generally. Given the significant increase in disclosure and subsequent use of exploits targeting external-facing appliances such as VPN concentrators, network defenders should anticipate rapid moves by a variety of adversaries, whether related to DarkSide or not, to take advantage of such potential ingress points.

Lateral Movement and Command and Control Activity

Once within victim networks, DarkSide-related intrusions leverage a combination of built-in system tools (such as "LoLBins") and publicly or commercially available tools for varying levels of network communication and functionality. Such items are deployed to both spread throughout the victim network, as well as to maintain command and control (C2) over any implants or tools. Examples include:

- The Sysinternals remote command execution utility PSExec
- Commercially available remote access tools such as TeamViewer
- The PuTTY-related application Plink
- The commercially available (but frequently pirated or cracked) Cobalt Strike
- The publicly available Custom Command and Control (C3) framework
- Network enumeration tools such as ADRecon and BloodHound for mapping victim Active Directory instances
- Tunneling C2 traffic, including RDP, via The Onion Router (TOR) to mask activity

Additionally, adversaries leverage built-in tools such as RDP and Server Message Block (SMB) connections to enable tool or capability deployment and lateral movement in victim environments, combined with continuous credential harvesting via tools such as Mimikatz.

At this stage, endpoint-related visibility becomes valuable in assessing an intrusion in many cases. However, even the best endpoint visibility on its own is insufficient to track, detect, and monitor elusive adversaries. This is especially the case for internal network movement. By pairing network monitoring and visibility with robust network security monitoring, defenders can ensure that all possible avenues for intruder operation are accounted for.

Like the initial access vectors described in the previous section, the lateral movement and C2 mechanisms identified here are hardly unique to DarkSide deployment. Instead, these techniques encompass behaviors also deployed by entities ranging from APTs to other, criminal actors. By establishing monitoring for either external communication linked to the tools or techniques listed above, or examining internal communication flows for lateral movement activity, defenders can identify malicious behaviors even when endpoint and similar visibility can be evaded.

Data Exfiltration

One other component to DarkSide-related operations, along with some other ransomware families, is the use of “double extortion” to prompt payment. In addition to encrypting data, victim information is stolen with threat of publication unless payment is made. Identifying large-scale data exfiltration in progress can be an indicator of imminent disruptive actions, and if caught in time may allow for defenders to respond quickly to prevent further harm. Based on reporting from researchers at Red Canary on general trends in this space, as well as specific observations on DarkSide, the following tools and techniques appear associated with “double extortion” operations:

- Use of cross-platform, free tools such as Rclone or WinSCP
- Mega.io-focused tools such as MEGAcmd or MEGAsync

Although not conclusively proven, media reporting indicates at least in the Colonial incident the criminals leveraged cloud hosting infrastructure, specifically from Digital Ocean, as an intermediary for data exfiltration as part of this process.

The above behaviors provide a variety of potential detection possibilities. Examples include simple tracking of large, anomalous traffic flows indicative of large-scale data exfiltration to use of specific service and destination

combinations (such as WinSCP to an Autonomous System Number (ASN) associated with a cloud provider).

Network Visibility and Monitoring

The mechanisms identified above are not distinct to DarkSide deployment; this provides a substantial benefit to defenders in that identifying general techniques associated with such intrusions will enable defensive coverage over a wide number of potential adversaries. Moreover, given the efforts by DarkSide-related entities (as well as numerous other threats) to evade endpoint detection and response (EDR) solutions as part of fundamental tradecraft, bolstering host-centric visibility with robust network monitoring can enable organizations to detect such operations at multiple phases of the Cyber Kill Chain.

Establishing network visibility and monitoring not only at the network edge but also for internal network traffic can enable powerful defensive responses covering a variety of threats. Looking at the behaviors identified in the previous sections, various defense and alerting mechanisms emerge from initial access through lateral movement and code execution.

External Monitoring

Monitoring external scanning or authentication brute force activity can be difficult given the sheer volume of activity from multiple services, malicious actors, and other entities. Yet being able to differentiate security-significant “signal” from background “noise” is critical in articulating meaningful, sustainable network defense.

For example, identifying exploit scanning activity, such as for the VPN vulnerability linked to DarkSide deployment above, may rapidly result in numerous alarms for various commercial or academic scanners attempting to identify vulnerable instances. Instead of attempting to chase every single potential vulnerability scan, defenders should seek higher-quality, lower-volume detections to ensure focused and efficient operations.

By viewing network security events not as atomic, discrete objects but as interrelated items linked through time and execution, powerful possibilities emerge for detection and analysis. For example, identifying linked activity such as a vulnerability scan of an external-facing service (or an explicit attempt to exploit that service) followed by scanning or authentication activity from that victim host to other, internal hosts within the network can flag likely initial intrusion actions and adversary attempts to expand access. By linking the discrete observations into a complex, high-confidence analytic of malicious behavior, defenders can not only ensure response to only high-severity, high-confidence events, but also alert on tradecraft linked to numerous threat actors.

Similar methodologies apply to credential stuffing, brute force, or guessing activity. Again, a variety of scanners and other items will likely be engaged in such activity on a daily basis. But identifying instances of dedicated scanning or brute forcing from a single source, or such activity followed by anomalous network traffic from the recipient of such activity, can narrow observations to likely compromise scenarios. Defenders can then vector resources and efforts appropriately to these events to initiate incident response operations, minimizing time to detection and time to recovery.

Other possibilities exist related to specific services and protocols. For example, in DarkSide operations deploying parties tunnel RDP via TOR in order to mask operations. While evading attempts to identify external RDP connections, this still requires communication to TOR nodes. Tracking and identifying TOR nodes and related

traffic can serve as a potentially powerful way to either enable more robust monitoring or, if blocked, reduce network attack surface. Similarly, and as stated above, by identifying combinations of activity such as network traffic flows indicative of large-scale data movement or exfiltration to untrusted or unfamiliar network infrastructure or ASNs, key portions of the "double extortion" model can be flagged prior to completion.

Internal Network Communication

Network monitoring and defense does not end at the perimeter; to deal with current threats (whether criminal actors or APTs) such visibility and response must extend to internal network communications. By leveraging a visibility fabric or deploying dedicated sensors inside the perimeter to track host-to-host traffic and similar flows, defenders can gain valuable visibility into adversary behavior that can identify intrusions in progress that boundary monitoring or EDR solutions otherwise miss.

For example, DarkSide deployment, along with multiple other actor behaviors, frequently uses credential theft followed by mapping a share over SMB for file transfer, then execution, via a tool such as PSExec. Identifying the concrete behaviors behind this activity and establishing alerts when these events are identified in sequence (authentication to host, SMB share mapped to another host, followed by file transfer of an executable or scripting object to the newly mapped host) can reveal instances of lateral movement. While it is possible such actions could identify legitimate system administrator activity, in well-orchestrated environments such instances can be rapidly dispositioned, while the existence of an analytic identifying these linked network-specific events can flag actions related to a variety of threat actors.

Additional opportunities include monitoring of traffic flows and authentication activity, such as when an adversary deploys legitimate tools such as RDP. In these cases, identifying a number of attempted or successful authentication attempts from a single host to multiple hosts inside the network can indicate an adversary attempting to break out of an initial network foothold. Further visibility, including being able to track precisely what credentials or user accounts are used, can reveal compromised accounts and other valuable response information.

Overall, the goal is to establish a combination of visibility into internal network traffic flows and combine this with an understanding of adversary tradecraft and operations to produce high-confidence alerting on observed activity. When paired with external network monitoring and endpoint defense, network defenders can severely impede adversary operations, ensuring multiple potential detection points throughout the attacker's lifecycle.

What Role Does Gigamon Play in Ransomware Defense?

Network Traffic Visibility and Network Detection and Response

While SIEMs and EDRs have increased SOC and incident response (IR) team's effectiveness in identifying active infections, visibility gaps to devices, networks, and traffic remain. The result is that analysts are left in the dark when trying to identify all adversary activity described across the MITRE ATT&CK framework.

Gigamon Hawk Visibility and Analytics Fabric

At the heart of an effective security posture is visibility, which in this case means access to all network traffic. Gigamon visibility fabric collects and aggregates all data in motion and eliminates blind spots:

- Single point of access to any infrastructure: physical, virtual, and cloud, including container traffic
- Aggregation of traffic collected via physical and virtual TAPs across the network
- Flow Mapping®, GigaStream® traffic distribution, and base stripping and tunneling for sending traffic to any destination
- Inline Bypass and physical bypass for failsafe traffic access, traffic forwarding, and inline security tool operation
- Traffic transformation and optimization, such as packet de-duplication, NetFlow generation, packet and flow slicing, etc.

Gigamon TLS Decryption

Adversaries increasingly leverage SSL/TLS encrypted channels for C2 and similar activity, and many of the detection techniques mentioned above require access to decrypted traffic. Most Fortune 1000 companies and government agencies rely on Gigamon for TLS inspection:

- Decrypts once and shares with all security and monitoring tools, with support for automatic SSL and TLS detection on any TCP port, with 10 Mb to 100Gig interface support
- Strong crypto support including Diffie-Hellman Ephemeral, elliptic curves, Poly1305/ChaCha20
- All advanced ciphers, including TLS 1.3 with Perfect Forward Secrecy
- Diffie-Hellman Ephemeral, elliptic curves, Poly1305/ChaCha20 crypto
- Inline or man-in-the-middle, and passive or out-of-band decryption
- Policy-based selective decryption privacy and support for URL categorization and FIPS 140-2 Level 2 cert

Gigamon ThreatINSIGHT

The synergy between SSL/TLS inspection and network detection and response techniques is an effective means to combat this threat vector and regain visibility over adversary operations. Gigamon ThreatINSIGHT™ Guided-SaaS NDR is a technology built by incident responders, for incident responders, that:

- Provides near packet-level visibility and recording of:
  - Any device: Managed/unmanaged/IOT
  - Any networks: Core/cloud/remote WFH
  - Any traffic: North-South, East-West, and encrypted
- Delivers high-fidelity adversary detection methodology and techniques, and is
  - Efficient: High-fidelity and QA’d proprietary threat intelligence
  - Effective: ML and behavioral analysis of uniquely malicious activity
  - Crowdsourced: To discover hidden and emerging threats
- Includes threat context:
  - Enriched metadata with near packet-level context
  - Indexed for powerful searching and investigation

    - Flexible retention options of 7-, 30-, and unlimited-day options

- Embeds recommendations for analysts and responders:
    - Guided: Threat-specific next steps for response
    - Guided: Powerful threat hunting and full investigation/incident management workflows seek to extend their visibility beyond logs and frontline security alerts in SIEMS and beyond EDR solutions

Webinar on Ransomware

Join us on Tuesday, June 8 at 10 a.m. Pacific/1 p.m. Eastern for the Ransomware Loitering Presents an Opportunity for Network Detection webinar. Bassam Khan, VP of Product and Technical Marketing at Gigamon, will explore how ransomware loitering lets security analysts use network detection and response capabilities to discover malicious activity between initial compromise and encryption.

Register here >>
