Shedding Light on the DarkSide Ransomware Attack

securityintelligence.com/posts/darkside-oil-pipeline-ransomware-attack/

CISO May 10, 2021

By Limor Kessem 7 min read

It has been well over a decade since cybersecurity professionals began warning about both nation-state and financially motivated cyber-kinetic attacks. Concerned about a cybersecurity threat that would have the potential to destroy physical assets and human lives, many looked

to sound the alarm in industrial organizations, tracking the vulnerabilities that could lead to a compromise in operational technology networks.

A variety of attacks in that realm took place over the years, whether launched in nation-state conflicts across the globe or as an apparent amateur challenge. Most recently, cybercriminals who deploy ransomware targeted a large U.S. refined products pipeline system, causing disruption to its operations and making headlines across the world. The attack reportedly only affected IT networks but had the potential to spread to operational zones and upstream to the overall supply chain — an attack scenario that could be much more damaging.

Unlike many attacks on industrial organizations that have been connected to adversarial nation-states, it seems that the pipeline attack might be a cybercrime case motivated by a large bounty. The group suspected in this hit goes by the name “DarkSide.”

IBM Security X-Force data shows that ransomware has become the number one threat type X-Force responded to in 2020 accounting for 23% of actual attacks that impacted organizations. Of those, our incident response data shows 59% of attacks were double-extortion cases, where in addition to having their data encrypted, victims were also threatened with data being leaked unless they paid for a decryption key by a specified deadline.

X-Force incident response data further shows that ransomware attacks were the most common threat to organizations that use operational technology (OT) in 2020. Sectors we examined in our data include manufacturing, oil and gas, transportation, utilities, construction, and mining, where ransomware attacks accounted for 33% of all attacks we responded to. This trend suggests that threat actors may be finding organizations with OT networks to be particularly attractive for ransomware attacks precisely because of the costly downtime and impact on a wider ecosystem and on individual consumers.

Who is on the DarkSide?

In August 2020, a new ransomware gang announced its entry into the cybercrime arena. In no less than a “press release” of sorts, its operators declared they had developed the perfect ransomware tool because other codes they used in the past were not up to the task. The post appeared on the group’s TOR domain where the newcomers also advised they were not inexperienced cybercriminals and acted as former affiliates to other successful gangs, making millions of dollars in the process. The malware itself has small similarities to the GandCrab and Sodinokibi ransomware, as does the ransom note’s template. Another similarity is that DarkSide is designed to avoid computers where a language layout corresponds with one of 17 countries from the former Soviet Union, adding Syrian Arabic — another similarity to Sodinokibi. When looking for affiliates to join their ranks, tech-savvy Russian speakers need apply. They further stress that they are *not* interested in “English

speaking personalities." DarkSide has also noted that while they plan to target organizations, they would aim for those who 'can pay' and spare healthcare, schools, non-profits, and government.

New Group, Old TTPs

Like other gangs that operate modern ransomware codes, such as Sodinokibi and Maze, DarkSide blends crypto-locking data with data exfiltration and extortion. If they are not initially paid for a decryption key, the attackers threaten to publish confidential data they stole from the victim and post it on their dedicated website, DarkSide Leaks, for at least 6 months. When a ransom note appears on an encrypted networked device, the note also communicates a TOR URL to a page called "Your personal leak page" as part of the threat that if the ransom is not paid, data will be uploaded to that URL. Ransom is demanded in Bitcoin or Monero. If it is not paid by a specific initial deadline, the amount *doubles*.

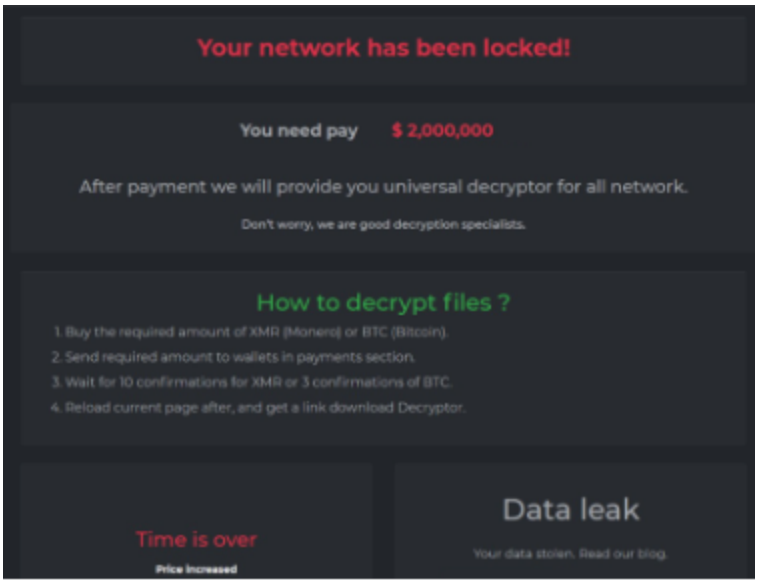


Figure 1: A "Welcome to the Dark" ransom note

A favorite entry point appears to be connecting via RDP on port 443 typically routing via a TOR browser. This is concurrent with a trend X-Force has been observing in similar attacks on organizational networks where attackers opt to scan and exploit targets rather than using compromised credentials.

Mimikatz and Cobalt Strike are part of the DarkSide attackers' arsenal. Used in post-exploitation, Cobalt Strike stagers help attackers control infected devices. 'Stagers' are tiny programs that download the larger Beacon payload and pass control to it.
Different parts of the attack are manually performed by an attacker, typically using familiar yet extensive living-off-the-land tactics. In cases of weakly secured or unmonitored servers, attackers were able to easily expand their ability to collect data and move laterally. Using Windows Active Directory tools, some cases lead to a DCSync attack that can end in the exposure of all AD data to the attacker and subsequent Golden Ticket attacks.

In various DarkSide attacks, systems, where an EDR solution was installed were avoided.

Need for Speed — DarkSide v2.0

Most ransomware operators understand that they need speed to encrypt as much data as possible as quickly as they can. They, therefore, opt to use symmetric encryption for that first phase and then encrypt the first key with an asymmetric key. In DarkSide's case, they claim to have come up with an accelerated implementation; the malware uses the Salsa20 stream cipher to encrypt victim data. They include an 80-byte public RSA-1024 key embedded in the malware's executable file and use it to encrypt the Salsa20 matrix. If implemented correctly, it is not possible to break this key and victims will have to find other ways to get their data back to an operational state.

Interestingly, to assure victimized organizations that they can make good on their decryption promises, DarkSide advertised their ability to provide the "fastest ever decryption speed."

The malware can attack both Windows and Linux environments, making enterprise servers just as 'encryptable' as an employee's endpoint. DarkSide can also attack virtual machines and encrypt data on their hard drives.

Where DarkSide attackers do take their time is the first stage of the attack. They do not initiate the encryption process until they have attained other objectives that can help them maximize eventual leverage on the victim, such as mapping networks and backups, setting up user access they can work with, and exfiltrating data they plan to leak later if they are not paid.

A Self-Confessed Financially Motivated Attack

The past decade saw ransomware evolve from a nuisance into one of the most impending risks CISOs and security leaders must reckon with, no matter the sector they operate within. The urgent need for incident response plans and capabilities has increased exponentially and has proven to be essential to mitigating risk, impact, and long-term results of cyber-attacks.

Disruption, extortion, and sometimes destruction are the hallmarks of cyber attackers out to demand a ransom, as the phenomenon grows over time. Ransomware attacks have been denounced and warned against by industry leaders and government officials alike. While addressing the U.S. Congress, former CISA director Chris Krebs noted that with raging ransomware attacks "we are on the cusp of a global digital pandemic driven by greed."

The group, when asked about their motivations, responded on social media that their aims were financial.

> “We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for other our motives.
>
> Our goal is to make money, and not creating problems for society.
>
> From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.”

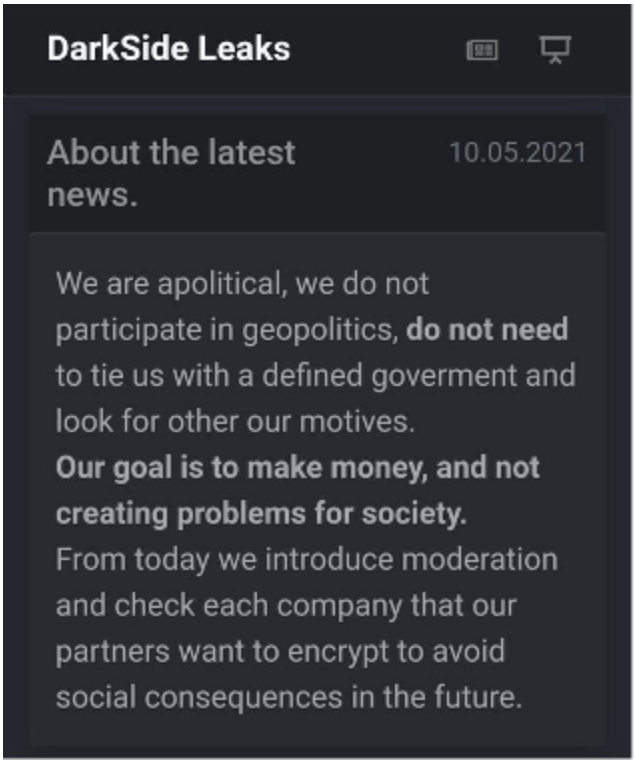


Figure 2: Source: DarkTrace

The growing number of ransomware incidents around the globe has made this a critical issue for national governments. As this attack continues to unfold, experts say fuel prices in the U.S. are likely to rise 2-3% starting May 10th, but the impact will continue to increase for as long as the pipeline is offline. A government-issued emergency waiver allows for the temporary delivery of fuel products via ground transportation until the pipeline’s operations are restored.

Adopting a Zero Trust Approach to Reduce Risk

Zero trust is a framework that assumes a complex network’s security is always at risk to external and internal threats. It helps organize and strategize a thorough approach to counter those threats.

By assuming that every connection and endpoint is considered a threat, a zero trust approach leans on a framework that protects against these threats, whether external or internal, even for those connections already inside. In a nutshell, a zero-trust network:

- Logs and inspects all corporate network traffic
- Limits and controls access to the network
- Verifies and secures network resources

To expand, the zero-trust security model is designed so that data and resources are inaccessible by default. Users can only access them on a limited basis under the right circumstances, known as least-privilege access. A zero-trust security model verifies and authorizes every connection, such as when a user connects to an application or software, to a data set via an application programming interface (API). It requires that the interaction meets the conditional requirements of the organization's security policies. A zero-trust security strategy also authenticates and authorizes every device, network flow, and connection based on dynamic policies, using context from as many data sources as possible. Learn more about IBM Security's zero trust approach.

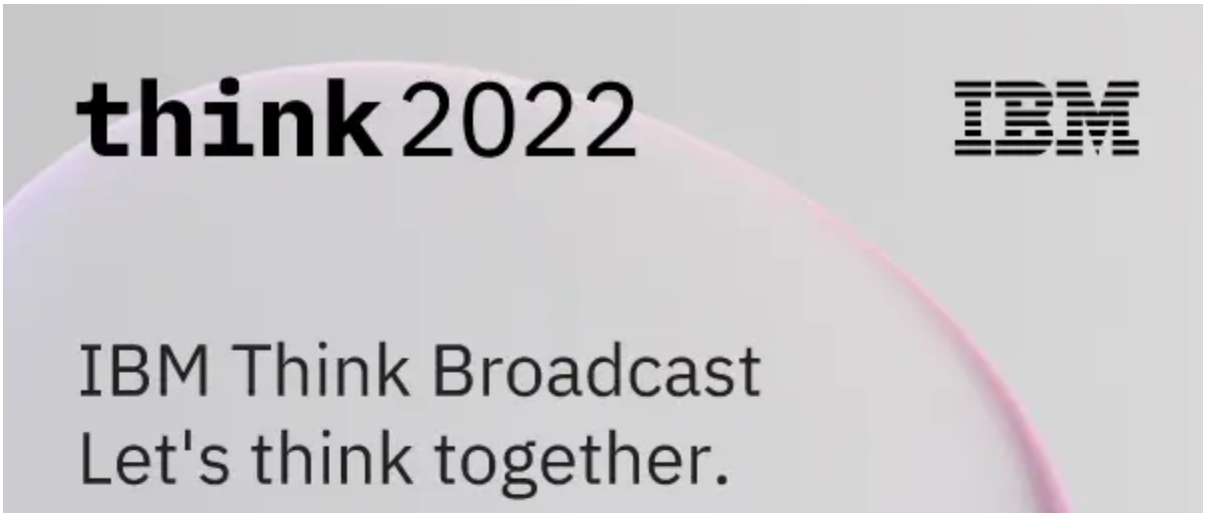
X-Force is advising organizations to be on alert for growing ransomware attacks and to be prepared with offline backups while implementing network segmentation and applying critical patches to reduce the risk. Companies also need to test detection capabilities with adversary simulation and red teaming, as well as rehearse and test incident response plans to identify gaps, so they can limit the spread of an attack if and when one happens. If you have more questions, join us on Thursday for our webinar on **U.S. Pipeline Ransomware Attack: IoCs, Attack Paths, Prevention** and download the IBM Ransomware response guide, and for ongoing updates on this situation check out X-Force Exchange.

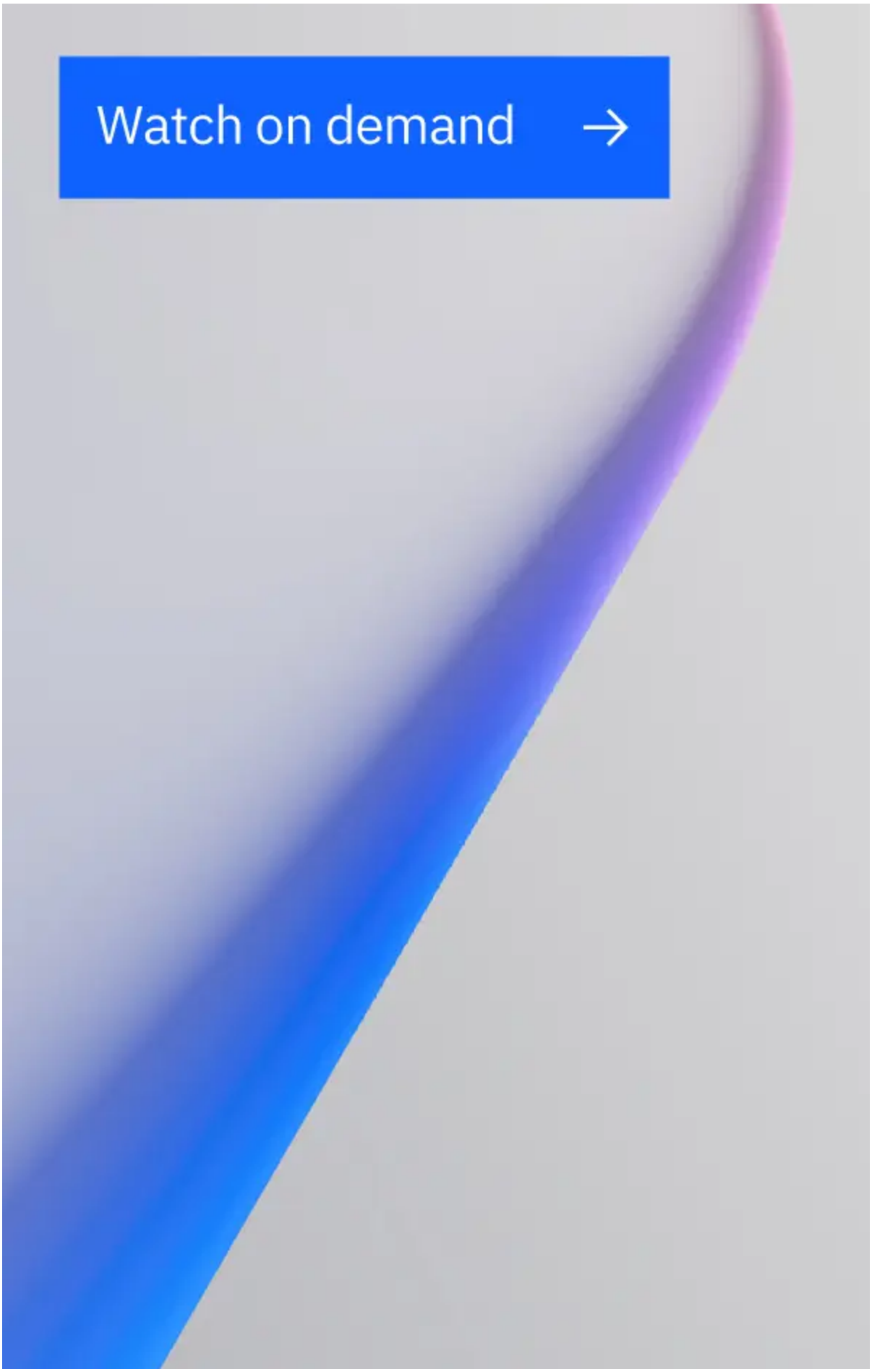
If your organization requires immediate assistance with incident response, please contact IBM Security X-Force's US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

Ransomware | X-Force

Limor Kessem
Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...




Watch on demand