DarkSide: The new ransomware group behind highly targeted attacks

digitalshadows.com/blog-and-research/darkside-the-new-ransomware-group-behind-highly-targeted-attacks/

September 22, 2020

We've recently observed the emergence of a new ransomware operation named DarkSide. The nuance of the operation includes corporate-like methods and customized ransomware executables, which have made headlines. When it comes to analyzing new ransomware campaigns, one might ask, "how innovative is this threat compared to previous ones?" Well, DarkSide is no different from its counterparts but is indeed the latest representation of the rising Ransomware-as-a-Corporation (RaaC) trend. Cybercriminals have seen their revenues steadily increase in the last years, making the ransomware market extremely prolific. Consequently, we've observed frequent attempts from threat actors to upscale their operations' external appearance to improve their reliability and reputation.

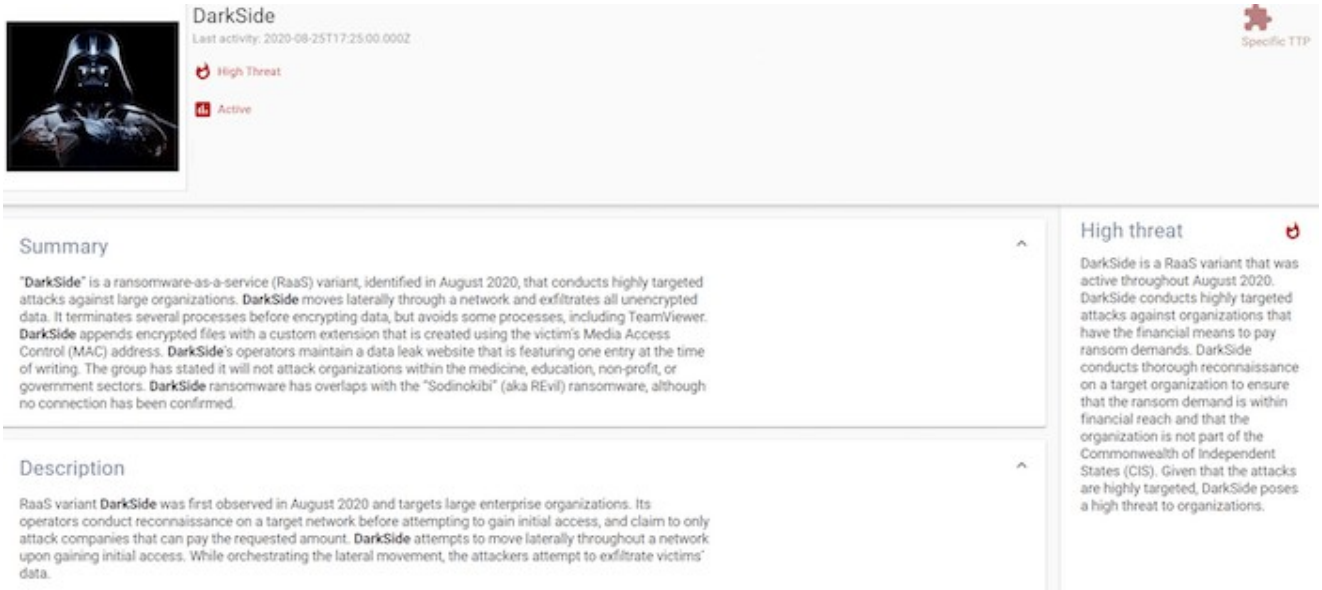

Figure 1: DarkSide threat actor profile in Digital Shadows' client portal

In the past month, Digital Shadows has been closely monitoring DarkSide, owing to their recent operation premiere and the interesting methods they utilize throughout their campaign. Since the threat intelligence nerds at Digital Shadows find this new operation so fascinating, we wanted to create a blog to detail our findings.

With that said, come with us to the *DarkSide* (see what we did there?) to get the skinny on our recent discoveries.

Bringing DarkSide to light

The DarkSide operation is hardly innovating in terms of tactics, techniques, and procedures (TTPs) used by other threat actors. The group shares its methods with infamous names like DoppelPaymer, Sodinokibi, Maze, and NetWalker. Many researchers that have analyzed the DarkSide ransomware agree that there are significant overlaps between this operation and those mentioned above. What, then, makes DarkSide particularly interesting? The answer is threefold:

1. The group has a highly targeted approach to targeting their victims
2. Custom ransomware executables are carefully prepared for each target
3. There is a corporate-like method of communication throughout their attacks

The group behind DarkSide announced its new ransomware operation via a press release on their Tor domain in August 2020. Up until this point, some researchers have claimed that the group has earned over one million USD; however, Digital Shadows cannot corroborate a definite figure at the time of this report. Possibly in an attempt to underline their experience, they made a point to clarify that the DarkSide operation isn't their first criminal experience; the campaign was developed to refine existing products into the ultimate ransomware tool.

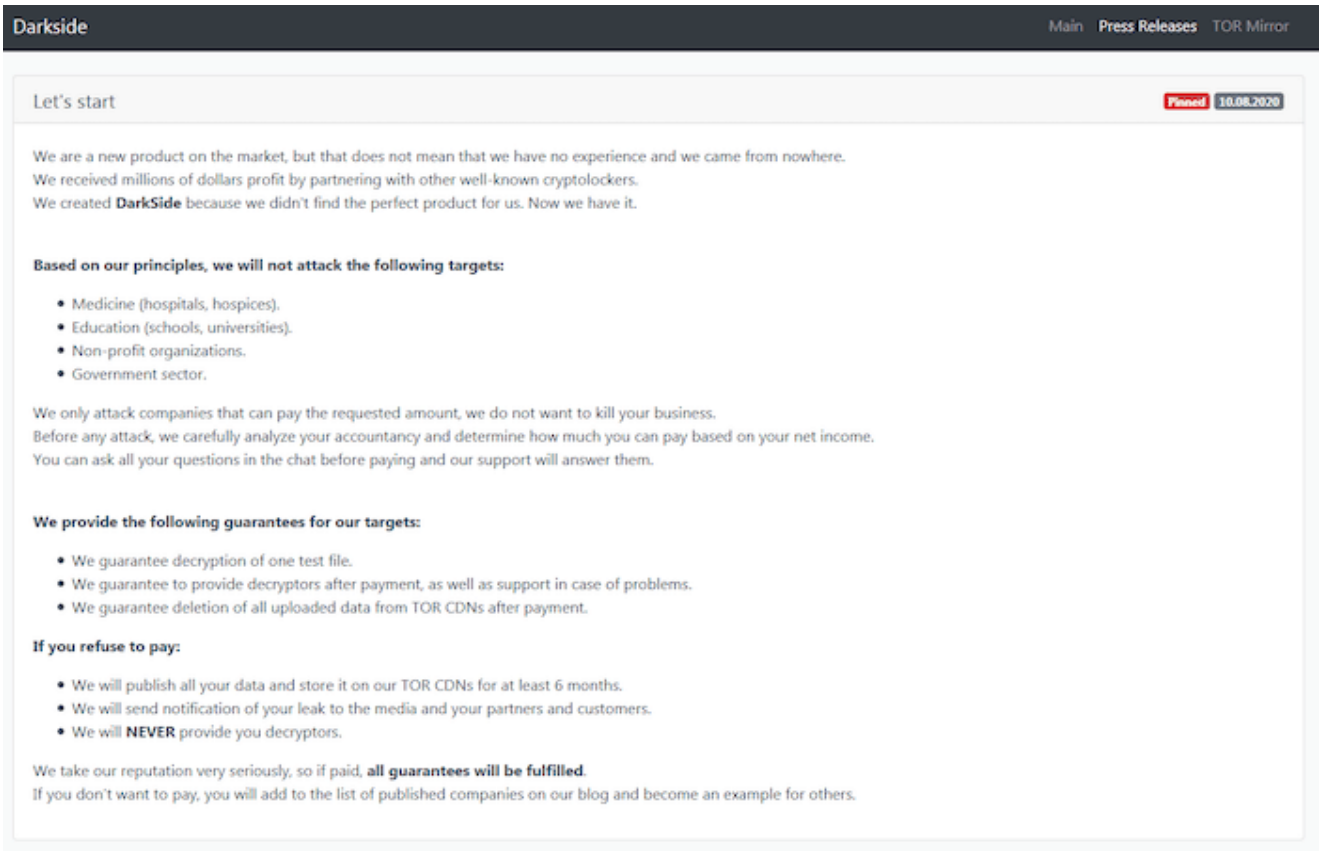

Figure 2: DarkSide press release announcing a new ransomware campaign

The press release stated several ethical principles that guide the group's decision process regarding their potential targets; they claim that the DarkSide operation will never target critical and vulnerable bodies such as schools, hospitals, or even governments. We've seen other groups claim to stay away from specific sectors (ahem… Maze); however, a recently unattributed ransomware attack, which targeted Duesseldorf University Hospital, may have

inadvertently caused a woman to lose her life. With these tragic concerns in mind, we'll see if they stick to their plan. To go even further, the group behind DarkSide states their intent to select their targets based on their financial revenue. This method implies that a ransom price is modeled around the victim organization's net income.

The operators behind DarkSide harvest the clear text data from their victim's server before encrypting it and requesting a ransom. The stolen data is then uploaded to DarkSide's leak website, which serves as a powerful extortion tool for the threat group. The targeted company risks sensitive data loss after a successful attack, and not to mention, a public breach can severely damage an organization's reputation. If this tactic sounds familiar to you, you're right on the money – we've been closely following the pay-or-get-breached trend since late 2019.

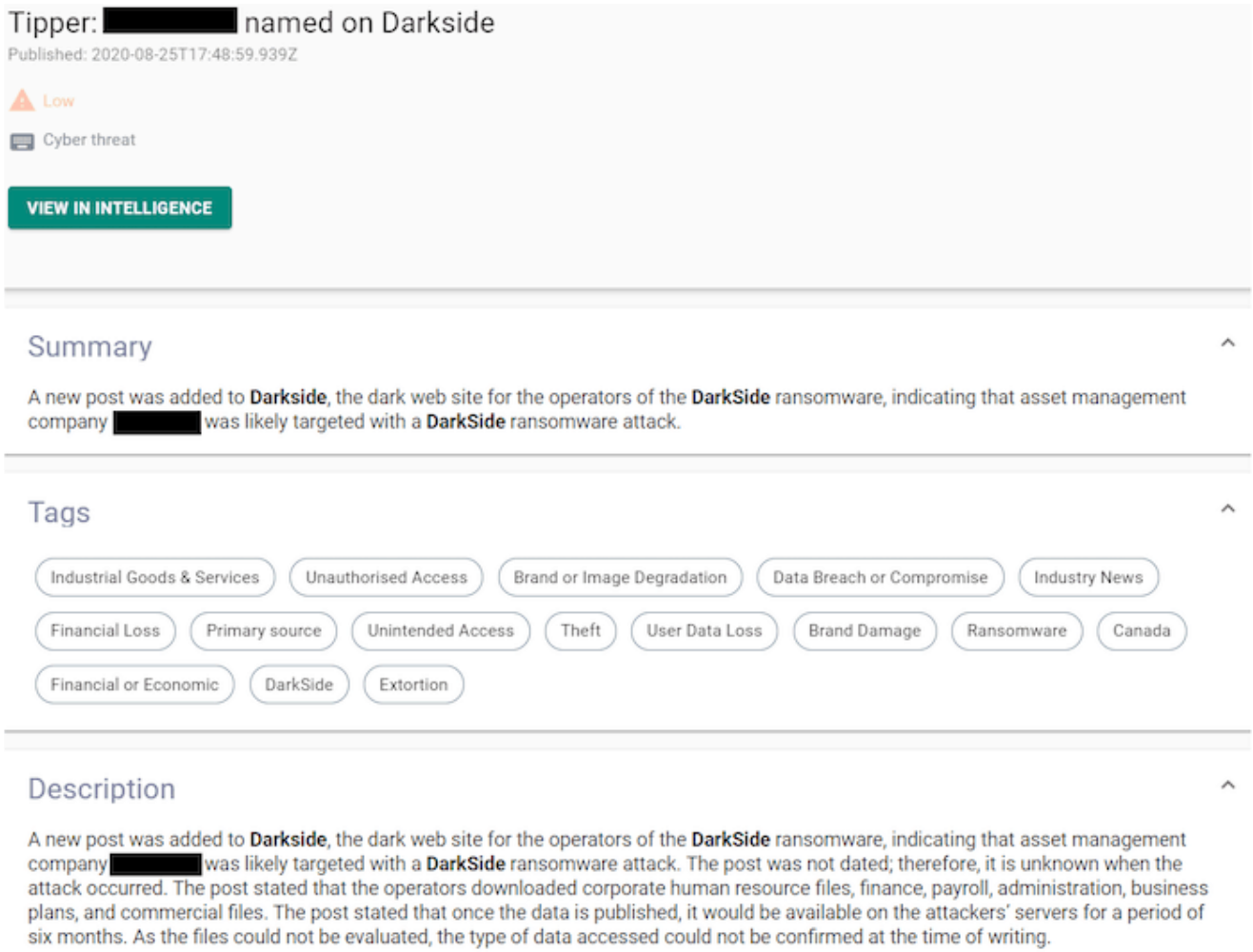

Figure 3: Digital Shadows intelligence alert about an organization affected by DarkSide

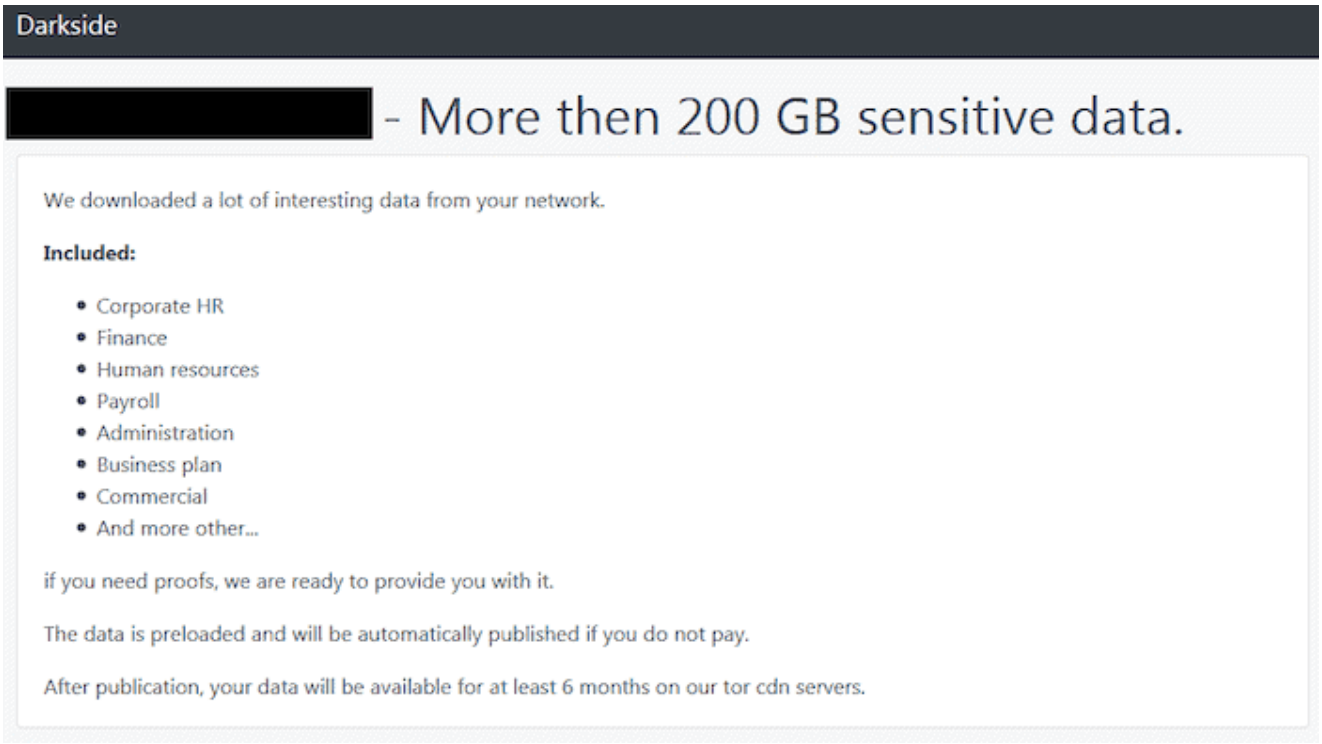

Figure 4: DarkSide exfiltration and encryption claims on their dark website

They're only interested in stealing from the rich

As we mentioned earlier, other ransomware operators have claimed to remove specific sectors from their attack itinerary. DarkSide's claim to avoid attacking companies within the education, healthcare, and government sectors can appear professional and respectable. Nonetheless, some promises are broken, and it is yet to be seen whether DarkSide will maintain its stated intentions.

DarkSide has additionally claimed that they choose their targets and determine a suitable ransom based on an organization's financial revenue. It's unconfirmed where DarkSide sources their organizational finance information from; however, Digital Shadows has found that, like many other ransomware operators, they may leverage relevant details from ZoomInfo.

Upping the ante with customized ransomware executables

DarkSide's operators customize the ransomware executable for the specific company they are attacking, indicating that they customize each attack for maximum effectiveness. The ransomware executes a PowerShell command that deletes Shadow Volume Copies on the system. DarkSide then proceeds to terminate various databases, applications, and mail clients to prepare for encryption. However, the following processes are avoided:

- Vmcompute.exe
- Vmms.exe
- Vmwp.exe

- Svchost.exe
- TeamViewer.exe
- Explorer.exe

Although unconfirmed, it is realistically possible that the operators use TeamViewer for remote access to computers, as it is rare that this process would be avoided.

Each customized executable includes a personalized ransom note, which consists of the amount of data that was stolen, the type of data, and a link to the data on the group's data leak site, where victims' information is leaked if a ransom demand is not met. While the site only references one compromised organization at the time of this blog, we plan to keep an eye on this group. In the meantime, we have listed DarkSide's current indicators of compromise (IoCs) and their associated MITRE ATT&CK techniques at the end of this blog.

Press releases make it look more professional, right?

DarkSide attempts to build trust with the victim and the other actors involved by leveraging professional communication methods. Over time, we have found that trust plays a pivotal role in the cybercriminal world and often determines the possibilities of an entity's growth and expansion. For example, the English-language marketplace, Empire, had long represented a trust stronghold on the dark web, favoring its establishment in the underground scene – until recently, when rumors of a possible exit scam started to circulate and gain increasing traction.

The use of a press release to announce a new ransomware operation is a symbol of the threat actor's intentions and maintains a dual-use:

1. Usually, only corporations and institutions use press releases; they project the impression of dealing with a professional body. In this case, a press release may convince the victim to trust the threat actor and pay the requested ransom.
2. Press releases attract media attention and ultimately weaponize stolen data, leading to severe reputational damage to a targeted organization.

This operation isn't the first time a threat group has used a press release to communicate its latest operations or threaten a victim. Many of us remember the campaigns conducted by "thedarkoverlord" in 2016 and 2017, which leveraged press releases in the wake of their attacks. Even more recently, in May 2020, REvil ransomware operators posted press releases to pressure their victims, which overtly named the compromised organizations and claimed to double their ransoms.

For press #1

Little press release. We worked closely with coveware on many data recovery cases. But something went wrong yesterday.
A case with some company was agreed for $7,500,000
At the very last moment, when we had already agreed on everything and were waiting for payment, coveware wrote that the client refused. We do not know how true this is, but the result in such cases is always the same.
Next. The hottest news, which we associate with [redacted]. Our demand was only 21.000.000$. The work was also done with the above mentioned coveware. After 10 days, we asked how much money had been collected from the amount. The answer was 365k. Of course, we realized that people are not determined to solve the problem. Correspondingly, our tactics the same:

1. The initial price of the contract is currently not valid and will be increased by the timer x2, as expected;
2. The data will be published every week in parts. It is inevitable and systematic. Up to the payment of the ransom up to a cent.
   Link: [redacted]
   Links are permanent and data update in the same place.

So, the ransom is now $42,000,000. They have that's the kind of money. And even more. But let's about nice one. After the publication, there was a report abuse on mega.nz. If once again there will be such reports - we rent 100 servers with fastflax and will make uploads. And at once on 3 steps forward, i.e. 3 archives on 100 gb forward. Lawsuits you will be pretty much, we guarantee it.

The next person we'll be publishing is Donald Trump. There's an election race going on, and we found a ton of dirty laundry on time. Mr. Trump, if you want to stay president, poke a sharp stick at the guys, otherwise you may forget this ambition forever. And to you voters, we can let you know that after such a publication, you certainly don't want to see him as president. Well, let's leave out the details. The deadline is one week.
Grubman, we will destroy your company to the ground if we don't see the money. Read the story of Travelex, it's very instructive. You repeating their scenario one to one.

And the new company that was attacked yesterday. We're not gonna name you yet, but just know that you have 24 hours to contact. Or you can be added to that honor list.

War to victory, only this way.

Figure 5: REvil ransomware operators' press release

Looking forward: Ransomware, Inc.

Although this operation displays a unique combination of tactics, communication, and ethical claims, DarkSide merely seems to be the latest product belonging to the growing trend of ransomware professionalization.

As RaaC continues to remain a popular method due to its rewarding financial return, we plan to see new threat groups with differing technical capabilities entering the ransomware Thunderdome. Whether or not they'll succeed in breaking the mold – only time will tell. While the cyber threat landscape can be unpredictable and volatile, a trend is a trend, and we will continue to monitor the cybercriminal bandwagon closely.

Indicators of Compromise (IoCs)

MD5: 1a1ea6418811d0dc0b4eea66f0d348f0

MD5: 25bb5ae5bb6a2201e980a590ef6be561

SHA256: 9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297

FILENAME: acer.exe

SHA1: d1dfe82775c1d698dd7861d6dfa1352a74551d35

MD5: f87a2e1c3d148a67eaeb696b1ab69133

FILEPATH: Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}

FILENAME: README.[victim's_ID].TXT

FILENAME: Win32 EXE

MITRE ATT&CK Techniques

Valid Accounts (T1078)

PowerShell (T1086)

System Services: Service Execution (T1569)

Account Manipulation (T1098)

Process Injection: Dynamic-link Library Injection (T1055)

Account Discovery (T1087)

Abuse Elevation Control Mechanism: Bypass User Access Control (T1548)

File Permissions Modification (T1222)

Data Encrypted for Impact (T1486)

Inhibit System Recovery (T1490)

System Information Discovery (T1082)

Process Discovery (T1057)

Screen Capture (T1113)

Compile After Delivery (T1500)

Service Execution (T1035)

Account Manipulation (T1098)

Credentials in Registry (T1214)

Tags: Cyber Threats / DarkSide / Ransomware