THREAT REPORT:

Six Ransomware Gangs Claim 290+ New Victims in 2021, Potentially Reaping $45M for the Hackers

Top Ransomware Operators Add Manufacturers, Transportation Companies and Construction Firms to Hit List

Every week, we read about a new company or public sector organization being attacked by ransomware. For example, in just the past two and half months, there has been ransomware attacks against:

- **Tata Steel** — compromised by Sodin/REdevil ransomware group in April 2021. Tata Steel refused to pay the $4 million ransom.
- **Broward County School District** — compromised by the Ryuk/Conti gang in March. Threat actors demanded $40 million, and the district said they would not pay.
- **Quanta Computer** — maker of Apple's next generation MacBooks attacked by Sodin/REdevil ransomware gang. Hackers demanded $50 million, first from Quanta who said no to the extortion, and then from Apple.

While we don't know if these three incidents reaped any ransom money for the perpetrators, we do know that ransomware operators are making plenty of money. Cyber-security company Emisoft estimates that the true global cost of ransomware, including business interruption and ransom payments in 2020, was a minimum of $42bn and a maximum of nearly $170bn. A survey by Veritas Technologies found that 66% of victims admitted to paying part or all of the ransom.

With so many ransomware incidents being reported by the press and by the hackers themselves (on their personal blog/leak sites), it's tempting to think you're fully aware of just how pervasive this threat has become. The reality is that the victim organizations we hear about publicly are a mere drop in the bucket compared to the actual incidents. One ransomware incident which occurred in April 2021, but which has never been made public, involved a small private U.S. company. The threat actors demanded $12 million and the company paid it, according to a high-ranking employee of the organization who asked not to be named.

In order to get a better handle on the true scope of ransomware, eSentire's security research team, the Threat Response Unit (TRU) decided to focus on the current activity of four of the top ransomware gangs and two emerging ransomware groups. Teaming up with Dark Web researcher Mike Mayes, the TRU and Mayes began tracking the Ryuk/Conti, Sodin/REvil, CLOP, and DoppelPaymer ransomware groups, and DarkSide and Avaddon, two emerging gangs.

TRU and Mayes found that specific groups not only racked up hundreds of victims in 2020, but they have collectively compromised 292 new victim organizations between January 1 and April 31, 2021, according to the groups' blog/leak sites. Palo Alto's research team, Unit 42, estimated in their 2021 ransomware report that the average ransom paid for organizations increased from US$115,123 in 2019 to $312,493 in 2020, a 171% year-over-year increase. Using the $312,493 ransom amount, and conservatively assuming only half of the purported victims paid the ransom, the total ransoms reaped by the six groups in the past four months is just over $45 million.

TRU and Mayes also found that these ransomware groups are not only continuing to target the usual suspects (state and local government, school districts, law firms, and hospital and healthcare organizations), but they have expanded their hit list to include manufacturers, transportation/logistics companies, and construction firms and not just in the U.S., but in Canada, South America, France and the U.K.

RYUK/CONTI

Number of victims listed	Recent victim profiles
352	• North America, the U.K., and France
New since Jan. 1, 2021	• Many manufacturers
63	• Several transportation/logistics companies and construction firms

TRU and Mayes also found that these ransomware groups are not only continuing to target the usual suspects (state and local government, school districts, law firms, and hospital and healthcare organizations), but they have expanded their hit list to include manufacturers, transportation/logistics companies, and construction firms and not just in the U.S., but in Canada, South America, France and the U.K.

The Ryuk/Conti ransomware group first appeared on the scene in August 2018. Their initial victims tended to be U.S.-based organizations, and they included technology companies, healthcare providers, educational institutions, financial services providers and numerous state and local government organizations.

In fact, the threat actors behind the Ryuk/Conti gang report they have hit a total of 352 organizations since coming onto the cybercrime scene, compromising 63 companies and private sector organizations this year alone. TRU examined 37 of Ryuk's 63 victims, and among them 16 were manufacturers. The manufacturers produce everything from medical devices to industrial furnaces to electromagnetic radiation equipment to school administration software.

Interestingly, of the 37 victims examined, TRU and Mayes found that only two have been made public — the Broward County School District and the CEE Schisler company. In March, Broward County was compromised by the Ryuk group. When they refused to pay the $40 million ransom, the hackers lowered their demands to $10 million, but the school system still refused to pay. As a result, the Ryuk group leaked 26,000 files (mostly financial, dealing with payments, invoices, etc.) belonging to the school district on their blog. The second victim was the French paper-cup manufacturer CEE Schisler, whose owner stated in a March 29 news article that they had not paid the ransom.

Other organizations Ryuk reports to have compromised in 2021 include transportation/logistics companies, construction companies, and healthcare organizations. Readers might recall that Ryuk made headlines in 2019 and 2020 with its successful attacks on several small U.S. communities, including Jackson County, Georgia, which paid a $400,000 ransom; Riviera Beach, Florida, which paid $594,000; and LaPorte County, Indiana, which paid $130,000. The Ryuk ransomware has also been seen in a wave of attacks targeting U.S. hospitals and health systems to the extent that the FBI and departments of **Homeland Security and Health and Human Services issued guidance to healthcare organizations.**

SODIN/REVIL

Number of victims listed	Recent victim profiles
161	• Primarily manufacturers, as well as a few healthcare organizations, transportation/logistic companies, and construction firms
New since Jan. 1, 2021	
52	

The Sodin/REvil ransomware group reports that they have compromised 161 victims since beginning their crime spree, 52 of which were in the first four months of 2021. Many of the businesses the Sodin gang claims to have hijacked this year are manufacturers, with the remaining victims including several healthcare organizations, transportation/logistics companies, and construction firms.

Two of the year's most notable ransomware attacks against manufacturers involved the Sodin threat group. In March, the group hit computer and electronics manufacturer Acer and demanded a $50 million ransom. Quanta Computer, which manufactures the Notebook computer, was another victim. As noted earlier, it was reported that the Sodin gang demanded $50 million from Quanta. The company refused to negotiate, and the Sodin criminals reportedly turned to Apple for the ransom. The Sodin hackers posted on their blog *"Happy Blog,"* a warning stating that if they did not get paid, they would publish what they claimed was technical details for current and future Apple hardware. The website 9to5Mac.com published several images of blueprints, which the Sodin threat actors claim are from Quanta. (See images 1-3)

The Sodin gang threatened to publish new data from Quanta every day leading up to May unless Apple agreed to pay the $50 million ransom in exchange for deleting the files. As of May 10, no additional documents appearing to be related to the Apple products have been leaked on Sodin's website. Interestingly, all images relating to the Quanta incident have been removed from Sodin's website, as well as any mention of the Quanta breach.

One writer was quoted as saying: *"Historically, Sodin isn't known for bluffing and routinely posts stolen documents if its victims don't pay up, so it's unclear why the group has failed to follow through on this occasion, and Apple has not commented on the breach thus far."*

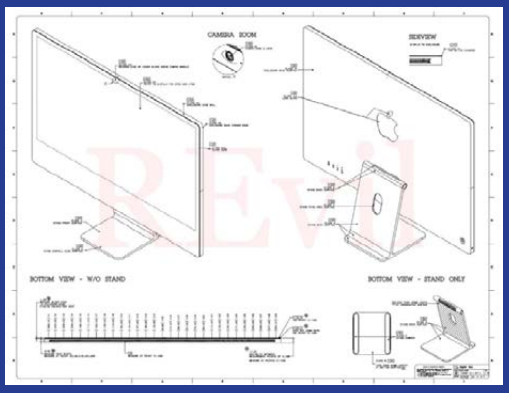

Image 1: Technical design of Apple hardware stolen from hardware manufacturer Quanta, according to Sodin

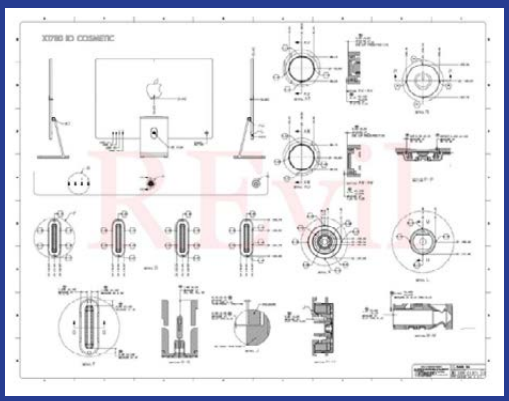

Image 2: Technical design of Apple hardware stolen from hardware manufacturer Quanta, according to Sodin

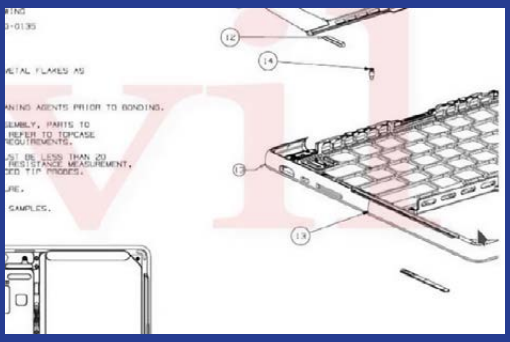

Image 3: Technical design of Apple hardware stolen from hardware manufacturer Quanta, according to Sodin

DOPPELPAYMER

Number of victims listed	Recent victim profiles
186	• Disproportionate number of government organizations (state and local municipalities)
New since Jan. 1, 2021	
59	

The DoppelPaymer ransomware group emerged in 2019 and is widely believed to be based on the BitPaymer ransomware, due to similarities in code, ransom notes, and payment portals.

In December 2020, the FBI issued a Private Industry Notification (PIN), DoppelPaymer Ransomware Attacks on Critical Infrastructure Impact Critical Services, warning that *"Since late August 2019, unidentified actors have used DoppelPaymer ransomware to encrypt data from victims within critical industries worldwide such as healthcare, emergency services, and education, interrupting citizens' access to services."*

The DoppelPaymer group reports on their website that they have compromised 186 victims since making their debut with 59 in 2021 alone. The victims include numerous state and local government organizations, plus several educational institutions.

Many of the small and medium businesses they claim to have hit have never been reported in the press, nor have many of the public sector entities. One of the exceptions is the Illinois Attorney General's Office, which first discovered the DoppelPaymer attack on April 10, 2021.

CLOP (Cl0p)

Number of victims listed	Recent victim profiles
53	• Manufacturers, retailers, financial organizations, law firms, and educational institutions
New since Jan. 1, 2021	
35	

The Clop ransomware was first seen in February 2019 and rose to prominence in October 2020, when the operators behind Clop became the first group to demand a ransom of more than $20 million dollars. The victim, the German tech firm Software AG, refused to pay.

Several of Clop's 2021 victims are reported to be the result of the supply chain attack against Accellion, a company that provides a file transfer application to companies around the world. It is not known if the Clop gang was behind the cyberattack against Accellion or if the Clop operators were given access to the data by the Accellion hackers. Regardless, Clop claims to have gotten their hands on data from Dutch oil giant Royal Shell, security company Qualys, U.S. bank Flagstar, global law firm Jones Day, University of Colorado, University of Miami, Canadian jet manufacturer Bombardier, Stanford University, the University of California, among others.

In early April 2021, Clop threat actors tried to extort RaceTrac Petroleum, another Accellion victim. RaceTrac is an Atlanta-based company that operates more than 650 retail gasoline convenience stores in 12 southeastern states. According to a statement made on RaceTrac's website, the Clop threat actors gained access to some of the company's Rewards Loyalty users' data: *"By exploiting a previously undetected software vulnerability, unauthorized parties were able to access a subset of RaceTrac data stored in the Accellion File Transfer Service, including email addresses and first names of some of the company's RaceTrac Rewards Loyalty users."*

Clop made headlines in 2021 for their tactic of culling through victims' stolen data and retrieving contact information for the company's customers and partners, then emailing them urging them to make the victim company pay the ransom. Clop operators' emails typically say that the recipient is being contacted because they are a customer of the victim organization, and their personal data, including phone numbers, email addresses, and financial information, will soon be leaked on a Dark Web site if the company does not pay the ransom. This note was published by security reporter Brian Krebs and is said to be a message sent to a RaceTrac rewards member. (See image 4)

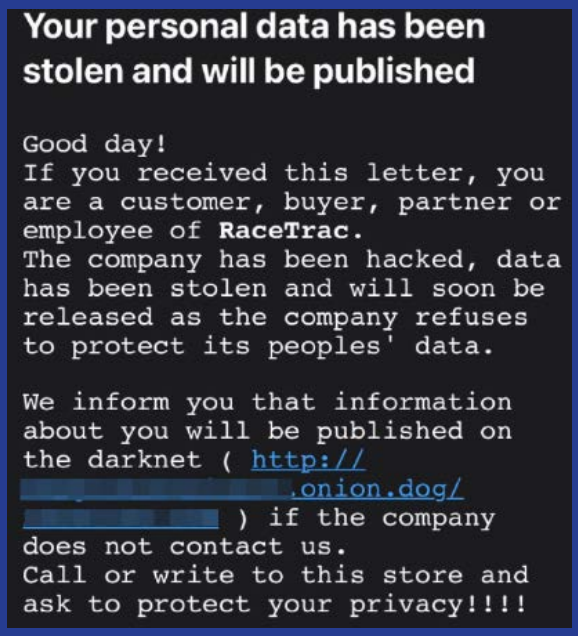

Image 4: Note from the Clop ransomware gang to a member of the RaceTrac rewards club.

Another retailer that Clop claimed to have compromised is grocery chain Foodland. Pacific Business News reported in early April 2021 that a similar incident occurred with customers of the supermarket chain to that of customers of RaceTrac Petroleum. According to the news outlet, an email was sent to Foodland customers from a suspicious email address and informed *"buyers, partners, employees and owners of Foodland that confidential information such as names, addresses, social security numbers, phone numbers and email was stolen."* Lawyers for Foodland Supermarkets Limited issued a April 23, 2021 notification of a data breach, due to a ransomware attack, which was said to have occurred on April 3. Clop claimed on their blog/leak site that Foodland was one of their victims. Foodland is Hawaii's largest locally owned and operated grocery retailers. The chain has 33 stores and more than 2,600 employees.

DARKSIDE

Number of victims listed	Recent victim profiles
59	• Victims located in the U.S., South America, Middle East, and U.K., and include manufacturers of all types of products, such as energy companies, clothing companies, travel companies
New since Jan. 1, 2021	
37	

DarkSide is a relatively new ransomware group. eSentire's security research team, the Threat Response Unit (TRU), began tracking them in December 2020, and the group is thought to have emerged in November 2020. The operators claim on their blog/leak site to have infected 59 organizations in total, compromising 37 of them in 2021.

News broke on May 9, 2021, that the DarkSide group might be behind the ransomware attack which forced the shutdown of Colonial Pipleline. On May 10, the FBI confirmed that the threat group was behind the attack. The Colonial Pipeline is one of the largest pipelines in the U.S. and delivers about 45 percent of the fuel used along the Eastern Seaboard. As of May 12, the shutdown caused gas shortages in many markets impacting hundreds of thousands of consumers. Late on May 13, the DarkSide blog/leak site went down with the DarkSide threat actors claiming that that it had lost access to the infrastructure it uses to run its operation and they would be closing, citing disruption from a law-enforcement agency and pressure from the U.S.

Prior to the DarkSide website going down, the operators always stated that they provided their malware via a Ransomware-as-a-Service model. eSentire's TRU has speculated whether one of DarkSide's affiliates (partners) was actually responsible for the attack against Colonial Pipeline, and that the threat actors behind DarkSide were, in fact, unaware of the sensitive target until news broke across the globe.

Interestingly, DarkSide published the following on their website on Monday, May 10, suggesting that this may be the case: *"We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for other 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."* (See image 5)

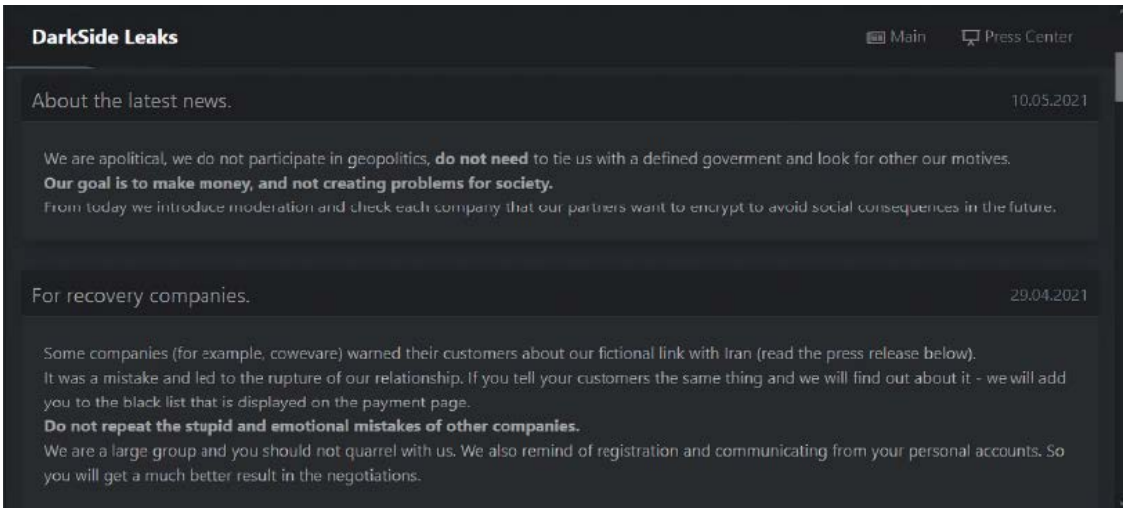

Image 5: A May 10 notification from the DarkSide operators on their website.

The DarkSide threat actors also bragged on their former blog/leak site that they were able to capture more of a foothold into their victims' IT environments, boasting that they seize victims' SQL databases, network passwords, network maps, any clear passwords and domain names.

DarkSide Continued to Claim New Victims after Colonial Pipeline Incident

Like many of the other ransomware gangs, the DarkSide operators would list their victims. Regardless of the tremendous attention paid to the DarkSide gang by law enforcement and security researchers, for several days following the attack on Colonial, they appeared to be carrying on as if it is business as usual. On May 11 and early on the 12, they posted two new victim organizations. One of them was a U.S.-based IT services company, from whom they claim to have stolen numerous types of data, including financial statements, employee passports, Active Directory passwords, etc.

The other purported victim is a UK-based civil engineering company that develops wind farms. From what TRU could ascertain from the DarkSide blog/leak site, it appears that their victims were primarily located in the U.S., South America, Middle East, and U.K. DarkSide victims include manufacturers of all types of products, clothing and office product retailers, law firms and travel companies.

Attacks against energy companies is not new to the DarkSide gang. In early February 2021, news broke that one of Brazil's largest electric utility companies, Companhia Paranaense de Energia (Copel), was hit by the DarkSide ransomware attack group. DarkSide also stated on their site on April 18, 2021 that they had compromised Georgia-based The Dixie Group (NASDAQ: DXYN.O). The Dixie Group manufactures carpets and custom rugs, and proprietary yarns used in manufacturing soft floorcoverings. eSentire cannot confirm DarkSide's claim that they compromised The Dixie Group. However, on April 19, The Dixie Group Inc., announced that they suffered a ransomware attack on their IT systems on April 17, 2021. News outlets also reported in March 2021 that the DarkSide operators attacked CompuCom Systems, gaining access to administrative credentials, and then deploying their ransomware.

Another purported victim of the DarkSide group is a well-known, US-based clothing manufacturer. Not only did DarkSide provide financial records that they claim are from the company, but they also provided video footage from what they claim is one of the clothing company's shipping and receiving centers.

They name other victims, as well, including a large company based in the Middle East that designs, manufactures, and markets a broad range of products for healthcare facilities; U.S. law firms; a large U.S.-based dental practice; a feed and fertilizer company; travel companies; and a sportswear company.

An ironic aspect of the DarkSide group is that they had registration sections on their blog for "press members" and "ransomware recovery firms." If you are a member of the press, they stated they would give you an exclusive, letting you know about a company that has been breached before they published it to their blog site. If you are with a ransomware recovery firm, they stated they would offer discounts on the ransom being demanded of the victim organization.

The DarkSide operators also liked to give the impression that they are like Robin Hood. They stated that they ONLY go after profitable companies — those organizations that can afford to pay a ransom. Further, they state that they will not attack hospitals, palliative care facilities, nursing homes, funeral homes, and companies involved in developing and distributing the COVID-19 vaccine. (See image 6)

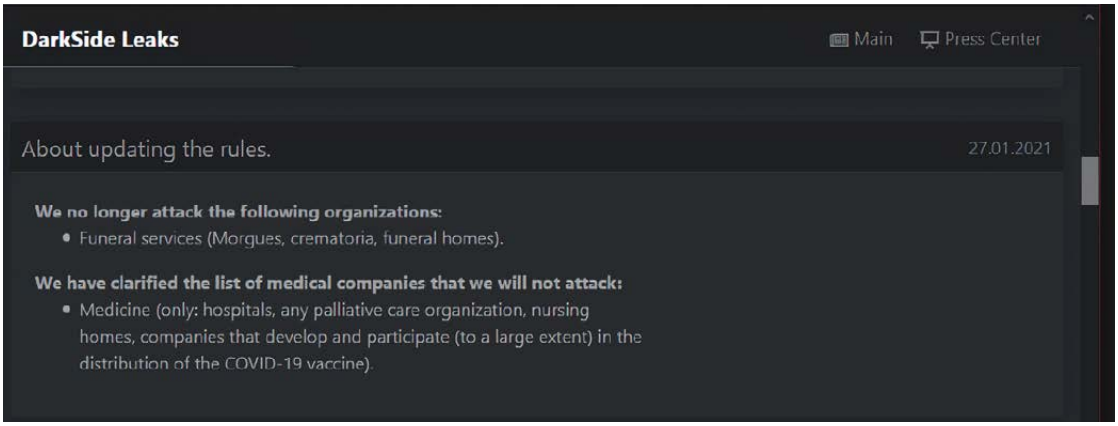

Image 6: DarkSide publishes on its website its "rules of engagement" regarding which organizations it will or will not attack.

Best of all, they state that they have donated $10,000 each to two charities in the United States. One of them focuses on providing education to disadvantaged children, while the other helps provide clean water to communities in Africa. The threat actors specifically ask that the names of the charities to which they have donated not be publicized so as not to cause the charities problems. (See Image 7)

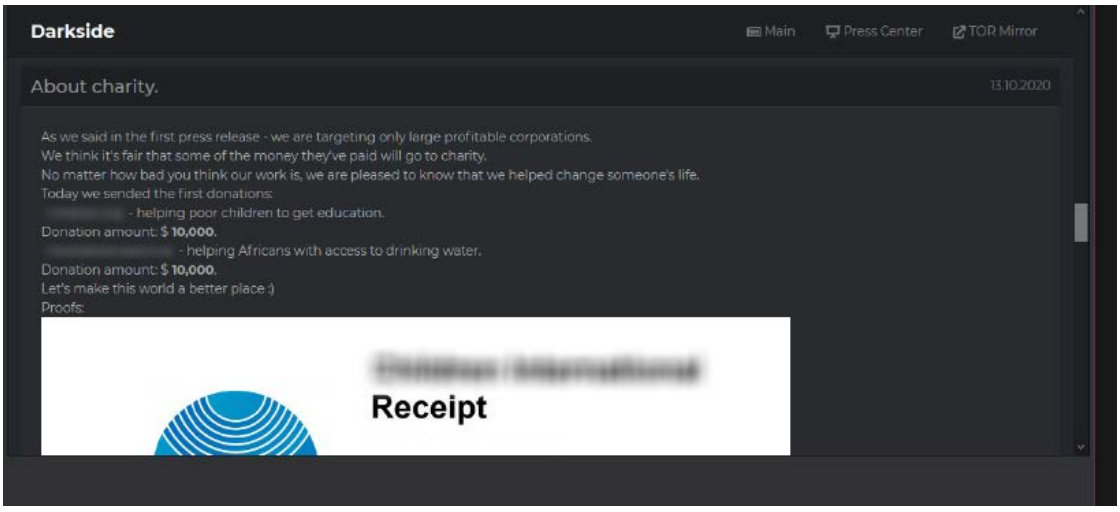

Image 7: DarkSide operators speak about the charitable donations they have made.

Finally, they offer to name the companies they have compromised in advance of publishing their names on their website so investors can earn money from the company's stock price reduction. (See image 8)

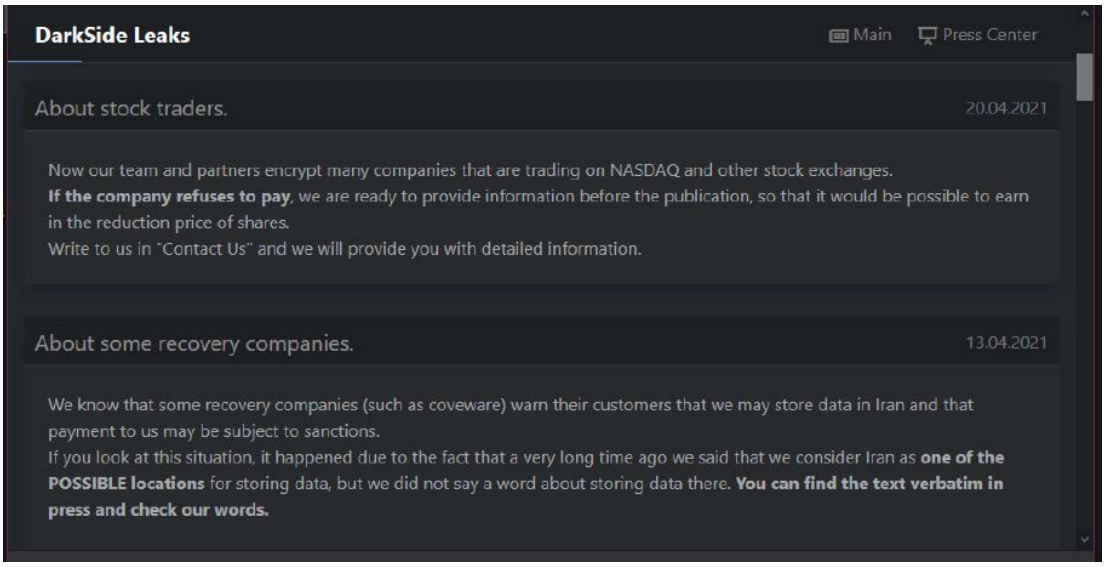

Image 8: DarkSide operators speak about the charitable donations they have made.

AVADDON

Number of victims listed	Recent victim profiles
88	• Numerous victims located in South America, Europe (especially in Italy and Romania), and Canada
New since Jan. 1, 2021	
47	

The Avaddon ransomware operators claim to have infected 88 victims during their lifetime, 47 of them in 2021. The ransomware was first spotted in the wild in February 2019 and is reported to be offered as a Ransomware-as-a-Service model. Its operators allow affiliates to use the ransomware with a portion of the profits paid to the Avaddon developers. The Avaddon threat actors are also said to offer their victims 24/7 support and resources on purchasing bitcoin, testing files for decryption, and other challenges that may hinder victims from paying the ransom.

What's interesting about this ransomware group is the design of its Dark Web blog site. They not only claim to provide full dumps of their victims' documents, but they also feature a Countdown Clock, showing how much time each victim has left to pay. And to further twist their victims' arms, they threaten to DDoS their website if they don't agree to pay immediately. The threat actors even go so far as to include a button next to each victim's name, indicating if their site is under attack. Talk about a 1-2-3 punch. At the end of April, the TRU Team confirmed that several of the victims' websites were down or slow to respond.

Unlike the DarkSide operators, the Avaddon threat actors and their affiliates don't have a problem attacking healthcare organizations. In 2021, news broke that they or their affiliates had compromised a number of healthcare entities and posted data allegedly stolen from their victims. These include the Capital Medical Center in Olympia, Washington, an intensive care online network, and Bridgeway Senior Healthcare in New Jersey.

Similar to the five other ransomware groups, Avaddon has also expanded its target list to include manufacturing and other private-sector entities around the globe.

Summary: How to Protect Yourself from a Ransomware Attack

The high-level of activity carried out by these six ransomware groups has certainly given the TRU team pause. If these threat groups are to be believed, they are wreaking havoc against many more entities than the public realizes. Another sobering realization is that no single industry is immune from this ransomware scourge. These debilitating attacks are happening across all regions and all sectors, and it is imperative that all companies and private-sector organizations implement security protections to mitigate the damages stemming from of a ransomware attack.

Below are a few basic security steps that every company should be employing to defend against ransomware attacks:

- Have a backup copy of all critical files and make sure they are offline backups. Backups connected to the infected systems will be useless in the event of a ransomware attack.
- Require multi-factor authentication to access your organization's virtual private network (VPN) or remote desktop protocol (RDP) services.
- Only allow administrators to access network appliances using a VPN service.
- Domain controllers are a key target for ransomware actors, so ensure that your security team has visibility into your IT networks using endpoint detection and response (EDR) agents and centralized logging on domain controllers (DCs) and other servers.
- Employ the principle of least privilege with staff members.
- Implement network segmentation.
- Disable RDP if not being used.
- Regularly patch systems, prioritizing your key IT systems.
- User-awareness training should be mandated for all company employees and focus on:
  - » Downloading and executing files from unverified sources
  - » Avoiding free versions of paid software
  - » Inspecting the full URL before downloading files to ensure it matches the source (e.g., Microsoft Teams should come from a Microsoft domain)
  - » Always inspecting file extensions. Do not trust the filetype logo alone. An executable file can be disguised as a PDF or office document.

Again, the most effective ransomware mitigation strategy comes in the form of offline backups. Unfortunately, victims rarely have reliable backups of key IT systems and data. When thinking about additional remediation measures, be sure to consider the following:

- Meet with your business teams to create an action plan and be sure to have an incident response (IR) plan mapped out that clearly defines which systems need to be put back online first.
- Prep your payment method. Nearly 75 percent of enterprises claim they would never seriously consider paying a ransom. When push comes to shove, more than 65 percent end up paying. Assume you'll pay, and establish cryptocurrency and prepaid voucher payment methods now. You don't want to waste precious time trying to set up a cryptocurrency account in the middle of an attack.
- Ready-set-go team. You need to create a reliable partner ecosystem well in advance of a breach. Not only is it important to have security vendor(s) in place to help prevent a ransomware infection, but it's vital that you have agreements already hammered out with a larger partner ecosystem, such as crisis communications agencies, digital forensic firms, cyber investigations teams, and outside counsel that specializes in security incidents.

If you're experiencing a security incident or breach contact us **1-866-579-2200**

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.