eSENTIRE

THREAT INTELLIGENCE REPORT

Grief Ransomware Gang Claims 41 New Victims, Targeting Manufacturers; Municipalities; And Service Companies in the U.K. And Europe

Grief Operators Earn an Estimated 8.5 Million British Pounds in 4 Months and Paralyze the 2nd Largest City in Greece & a Major Government District in Germany

Table of Contents

Key Findings

- The Grief Ransomware Gang (a rebrand of the DoppelPaymer Ransomware Group) claims 41 new victim organisations between May 27, 2021—October 1, 2021 with their ransomware.
- Over half the companies listed on Grief's underground leak site are based in the U.K. and Europe. The Grief Ransomware Gang appears to have altered its Modus Operandi (MO) targeting more corporate and public entities in the U.K. and Europe than the United States. They also seem to be backing away from U.S. hospitals and emergency healthcare services, previously a top target for them.
- Grief Victims in U.K. and Europe include a variety of manufacturers:
  - Those producing machinery for railways, sea harbours and shipyards
  - Manufacturers of food and beverages
  - Manufacturers of heavy construction materials
  - Manufacturers of fluid handling equipment for the oil and gas industry and the food industry
  - Manufacturers of computer hardware
  - Manufacturers of wood products
  - Manufacturers of feed for livestock
- Other U.K. and European-based Grief Victims include:
  - Multiple cities and towns in Europe, including the second largest city in Greece, Thessaloniki. This city has over a million residents. City leaders reported on July 23, 2021, that it had to shut down all its city services because of the attack. Also in July, the Grief threat actors hit the German government district of Anhalt-Bitterfeld with a debilitating ransomware attack. Anhalt-Bitterfeld is made up of 8 towns and 2 municipalities. Following the compromise, the region's leaders stated that the attack "almost completely paralyzed" the district's IT systems, estimating that their systems could be offline for a week or more. Because of the ransomware attack, the district was unable to pay out welfare benefits to recipients or finance youth programs. District leaders officially declared the incident a "disaster." With this declaration, Anhalt-Bitterfeld was able to get access to federal aid to help its 158,000 citizens and help restore its IT systems. Despite the damage caused by the Grief threat actors, they continued to attack municipalities, claiming the city of Porto Sant'Elpidio in Italy and the city of Villepinte in France as victims.
  - A national network of pharmacies
  - Large producers/growers of fruits and vegetables
  - Dairy producers
  - Providers of food services and hospitality services
- The Grief Gang has earned an estimated £8.39M (approximately £2.1 million per month), equaling €9.86M and $11.4M USD.
- Many of the corporations, municipalities and educational institutions listed on Grief's leak site have not been made public.
- The Grief hackers include on their leak site company name, web address and various documents reportedly belonging to the organisation. The Grief Gang posts these documents to serve as proof that they have compromised the organisations. The Grief gang also uses the exposed documents as a way of pressuring the victims to pay. It serves as a warning, that should the victims decide not to pay, Grief will expose more sensitive information. eSentire's Threat Response Unit (TRU) found that the documents exposed, many of them financial and HR- type documents, appear to be authentic.

Observations of the Grief Gang's Activities

Rob McLeod, VP of Threat Response Unit (TRU) - eSentire

"The Biden administration has increased pressure on other nations, primarily Russia, to rein in the cybercrime groups operating out of their jurisdictions. This focused attention could be the reason why the Grief Ransomware Gang is shifting their attention away from North America to target businesses and municipal governments in other wealthy Western markets, specifically the U.K. and Europe."

"The history of cybercrime is filled with examples where a threat group pretends to shut down and another one, with clear similarities in techniques, malware and targets, emerges a few months or even weeks after. We saw DoppelPaymer cease posting victims to their leak site in May, and suddenly the Grief ransomware leak site appears in June. If history is any guide, then businesses and government organisations (particularly, regional and local municipalities) in the U.K. and Europe should be on high alert. Already, more than half of Grief's victims are based in these markets."

"The TRU team found that among the 41 Grief victims, 5 are municipalities and one is a large government district consisting of 8 towns and 2 municipalities. That the Grief actors attacked such organisations doesn't surprise us, as this sector was a favorite target when the group went under the DoppelPaymer banner. Municipalities feels intense, immediate, and public pressure when their services are disrupted. The urgent need to restore services is a strong motivator to pay off attackers. Likewise, providing services is an essential requirement of a functioning government at all levels."

Note: Both municipal governments and educational institutions have been profitable for other ransomware groups, such as the Conti/Ryuk ransomware gang, which collected over a $1,000,000 from just three small U.S. municipalities prior to 2021. These included Jackson County, Georgia, which paid a $400,000 ransom; Riviera Beach, Florida, which paid $594,000; and LaPorte County, Indiana, which paid $130,000.

Introduction

The Grief Ransomware Gang (aka: PayOrGrief) claims to have infected 41 new victims between May 27, 2021—October 1, 2021, with their ransomware, according to eSentire's security research team, the Threat Response Unit (TRU). Cybersecurity researchers, including TRU, believe the Grief Group is merely a rebrand of the DoppelPaymer Ransomware Group. In its May 2021 Ransomware Report, eSentire found that the DoppelPaymer Gang was one of the most active ransomware groups, claiming to have infected 186 companies and public entities between 2019 and May 1, 2021. DoppelPaymer is considered one of the top ransomware groups, coming in just behind the Sodin/REvil, Conti/Ryuk, Black Matter (formerly Darkside) and CLOP groups.

When the Grief Group emerged on the ransomware scene at the end of May, TRU began tracking their activity and found that for the past four months they have been targeting multi-national corporations (especially manufacturers), municipalities, service organisations and school districts. Their victims are located across Europe, the U.K., the U.S. and Central America. However, TRU has observed that the Grief Ransomware Gang (formerly DoppelPaymer) has increased its focus on organisations in Europe and the U.K. specifically.

Of the 41 victims named by Grief, 22 of them are headquartered out of Europe or the U.K. The victims include numerous manufacturers, including those producing machinery for railways, sea harbours and shipyards, manufacturers of food and beverages; a manufacturer of fluid handling equipment for the oil and gas industry and the food industry; a manufacturer of computers, etc. Other victims include a national network of pharmacies, numerous municipalities, including Thessaloniki, the second largest city in Greece with over a million residents and the German district, Anhalt-Bitterfeld, which contains 8 separate towns and 2 municipalities.

Victims Named on Grief Leak Site (based in U.K. and Europe):

- Prominent producer of wine and champagne (France)
- Manufacturer of metal products (Italy)
- Manufacturer of wood products (Austria)
- Large national chain of retail pharmacies (Italy)
- Manufacturer of lumber and other construction materials (France)
- Longtime provider of hospitality services (U.K.)
- Large manufacturer of cranes used for harbours and shipyards (Germany)
- A large manufacturer of machines used for maintaining railroads and a provider of railroad maintenance services (Switzerland)
- A global supplier and manufacturer of solutions and fluid-handling equipment for the Oil & Gas and Food industry (France)
- A prominent global developer and manufacturer of computer hardware and IT solutions (Austria)
- A longtime manufacturer of feeds for animals (U.K.)
- A designer, developer, and manufacturer of high- end kitchen and bedroom furniture (U.K.)
- Thessaloniki, the second largest city in Greece. Thessaloniki has over a million residents (Greece)
- Anhalt-Bitterfeld, a government district in Germany, consisting of 8 towns and two municipalities (Germany)
- Porto Sant'Elpidio, a municipality in Italy (Italy)
- Villepinte, a municipality north of Paris (France)
- A decades-old catering services company providing catering to the public and private sectors (Portugal)
- An international developer and manager of oil palm and rubber plantations (France)
- A mid-size, modern manufacturer of food products, specialising in high-volume quality production, distributing their food products to major retailers, foodservice and manufacturing customers throughout the U.K. Europe and Middle East (U.K.)
- A manufacturer of food products for packaged foods, as well as fresh food, including a variety of meats (France)
- A large dairy producer (Austria)
- A producer of fruits and vegetables and manufacturer of specialty foods (Spain)

Other Grief Victims:

- An IT company specialized in cloud computing, data centers, IT outsourcing, service desk, and IT management (Brazil)
- A financial services company (Canada)
- Two municipalities (U.S.)
- Five separate school districts (U.S.)
- A provider of mental health and substance abuse rehabilitation services (U.S.)
- A corporation made up of businesses in the hospitality and transit industry (Dominican Republic)
- A large cotton cooperative (U.S.)
- A company which produces vegetables and fruits, with operations in California and Mexico (U.S.)
- A medical practice focused on dermatology and facial plastic surgery (U.S.)
- A manufacturer of ingredients for dessert making (Mexico)
- A 50-year-old + architectural, planning and interior design firm providing services to clients throughout the U.S. and internationally (U.S.)
- A large car and truck dealership (U.S.)

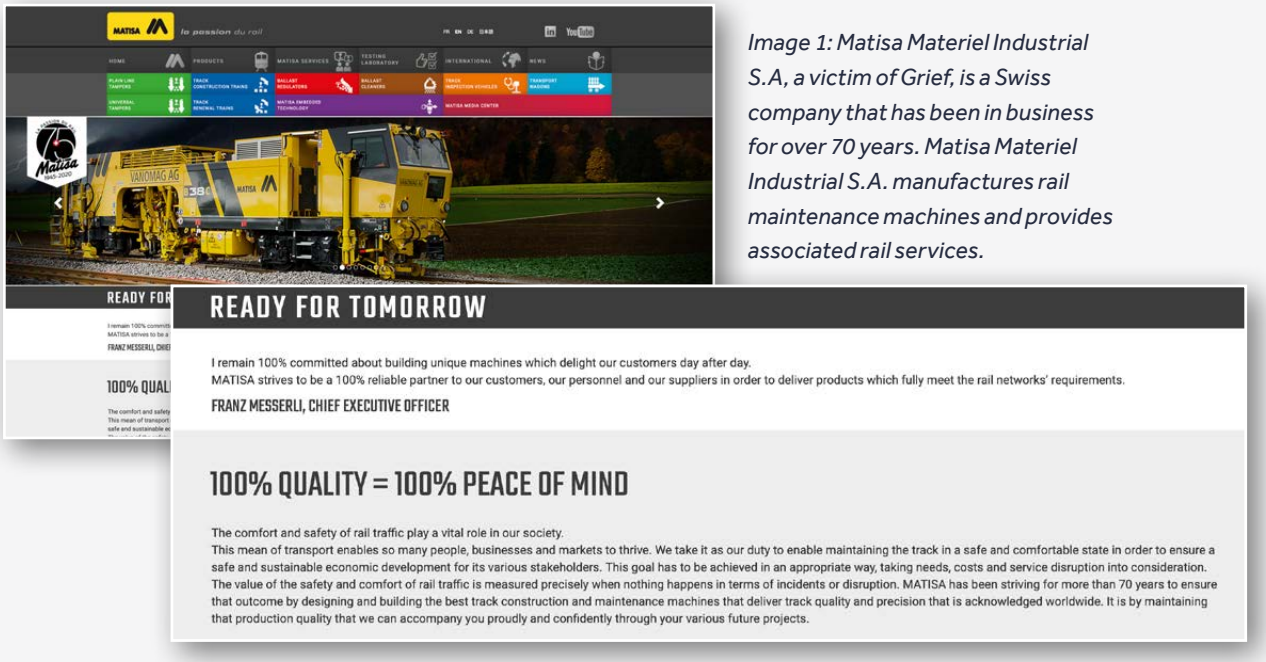

Image 1: Matisa Materiel Industrial S.A, a victim of Grief, is a Swiss company that has been in business for over 70 years. Matisa Materiel Industrial S.A. manufactures rail maintenance machines and provides associated rail services.

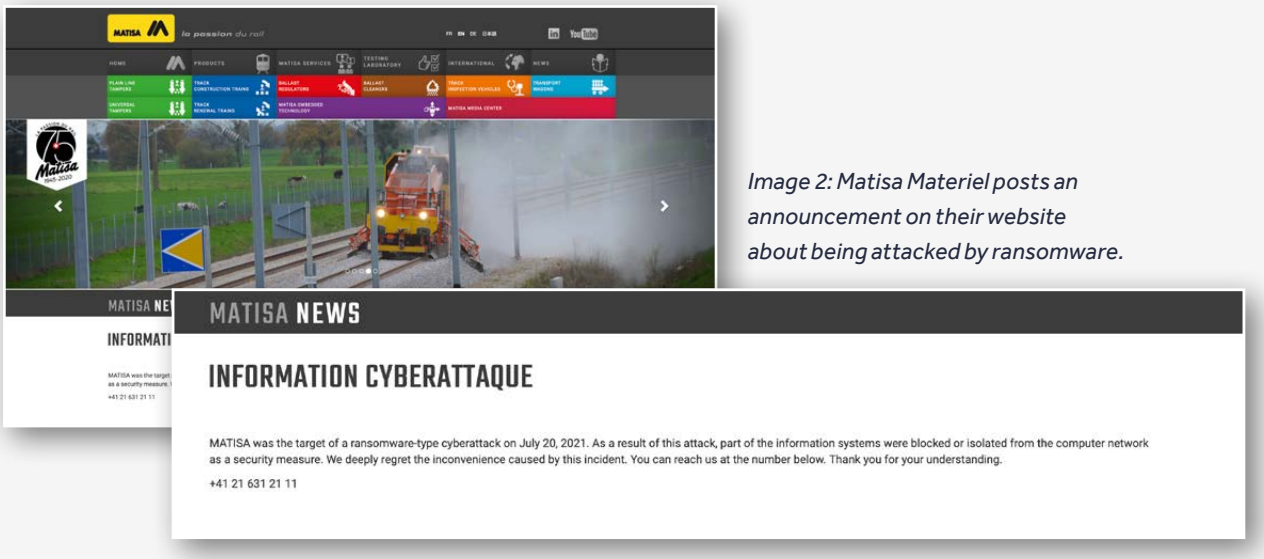

Image 2: Matisa Materiel posts an announcement on their website about being attacked by ransomware.

Potential Earnings of the Grief Ransomware Gang –June 1 to October 1, 2021

Grief claims to have hit 41 victims in just four months. Palo Alto's research team found that the average ransomware payment is up 82% in the first half of 2021, coming in at a record $570,000. Using the **$570,000** ransom amount, and conservatively assuming only half of the purported Grief victims paid the ransom, the total ransoms potentially earned by the Grief operators in just four months is approximately **£8.39M equal to €9.86M or equal to $11.4M USD**. That averages out at approximately £2.1 million per month.

While we don't know if all the manufacturers, municipalities, school systems and other entities, Grief claims as victims were compromised, typically eSentire does not see top ransomware operators, like Grief, fake a victim. And we do know that ransomware gangs are making plenty of money. A survey by Veritas Technologies found that 66% of victims admitted to paying part or all the ransom, and cybersecurity company **Emisoft** estimated 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. As we reported in our **May 2021 Ransomware Report** and it remains true, the victim organisations we hear about publicly are nominal compared to the actual ransomware incidents.

U.K. Cybersecurity Breaches Increase in 2021. Ransomware Incidents Increase Worldwide

As the United States applies pressure to other nations to rein in cybercrime gangs operating from within their borders, TRU is observing attackers increasingly targeting other wealthy Western nations in the United Kingdom and Europe.

Cyber Security Breaches Survey 2021, the most recent edition of a survey-driven report published annually by the U.K. government, found that, "Four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months." Other investigations found broadly consistent results. In August 2021 **Computer Weekly reported** that, "Accompanying the dramatic increase in ransomware attacks, organisations have also experienced a 29% increase in the number of cyberattacks globally, with the highest growth seen in the Europe Middle East and Africa (EMEA) region," at 36%.

Despite the well-documented increase in all kinds of cyberattacks—particularly ransomware—what is quite worrisome is another statistic brought out in the U.K. Cyber Security Breaches Survey. The authors of the survey reported, "fewer businesses are now deploying security monitoring tools (35% vs. 40% last year), and fewer businesses are undertaking any form of user monitoring (32% vs. 38%)." The survey's authors suggest that these decreases could be due to the added complexity of monitoring tools and employees in work-from-home environments (the 2020 report was based on pre-pandemic data, while 2021 was based on data and interviews spanning October 2020 to January 2021).

Ransomware operators, especially, have become very successful in recent years due in large part to **a maturing cybercrime ecosystem of specialised services**. The risk of real consequences for their actions is low, while the rewards are high, driving year-over-year increases of 93% in the number of ransomware incidents between 2020 and 2021, **according to a report by Check Point Software** and an 82% increase in the average ransom payment to $570,000, **according to Palo Alto**. These two trends converge to create a ransomware market in which **victims worldwide paid ransomware gangs more than $350M in cryptocurrency alone in 2020**. Unfortunately, a portion of these proceeds are reinvested into the ransomware 'machine' to fund an assortment of cybercrime operations, including research and development and—of course—more attacks.

While the ransom payments to restore services and the extortion payments to prevent the release of stolen information dominate headlines, the costs to victim organisations also include:

- The opportunity cost of redirecting scarce IT and security resources in response to the incident
- Loss of business or production due to service outages
- Reputational cost (which may have a long-lasting impact)
- Potential regulatory and contractual penalties
- Costs associated with third-party incident responders and investigators

Consequently, an attack need not generate revenue for the attacker for it to be incredibly costly for the victim organisations—so focusing on ransom and extortion payments alone substantially undercounts the true cost of cyberattacks.

Grief Hackers Taunt their Victims

The Grief hackers seem to enjoy taunting their victims. On Grief's underground leak site, they prominently post the victim company's name, company details and sample data stolen from the organisations. Ironically, the Grief gang also prominently displays various statistics around the cost of a data breach to a company, such as:

"Did you know that the cost of downtime is 10x higher than the ransom requested (per incident)?"

They display another cost statistic, from the Varonis 2018 Global Data Risk Report, on their leak site which reads:

"The average cost of a data breach in 2017 was over $3.5 million."

And they cite on their leak site, almost verbatim a portion of Article #33 of the General Data Protection Regulation (GDPR) rules:

"In the event of a personal data breach, data controllers, should notify the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it..." See image 3 on page 9.

In September, the Grief threat actors showed real displeasure about victims bringing in professional negotiators, publishing the following an edict on their leak site:

> *We wanna play a game. If we see professional negotiator from Recovery Company™ - we will just destroy the data. Recovery Company™ as we mentioned above will get paid either way. The strategy of Recovery Company™ is not to pay requested amount or to solve the case but to stall. So we have nothing to loose in this case. Just the time economy for all parties involved. What will this Recovery Companies™ earn when no ransom amount is set and data simply destroyed with zero chance of recovery? We think - millions of dollars. Clients will bring money for nothing. As usual.*
>
> Grief ransomware gang

Essentially, the Grief operators are saying that if a victim hires a negotiator, they will delete the victim's decryption key, making it impossible to recover their files.

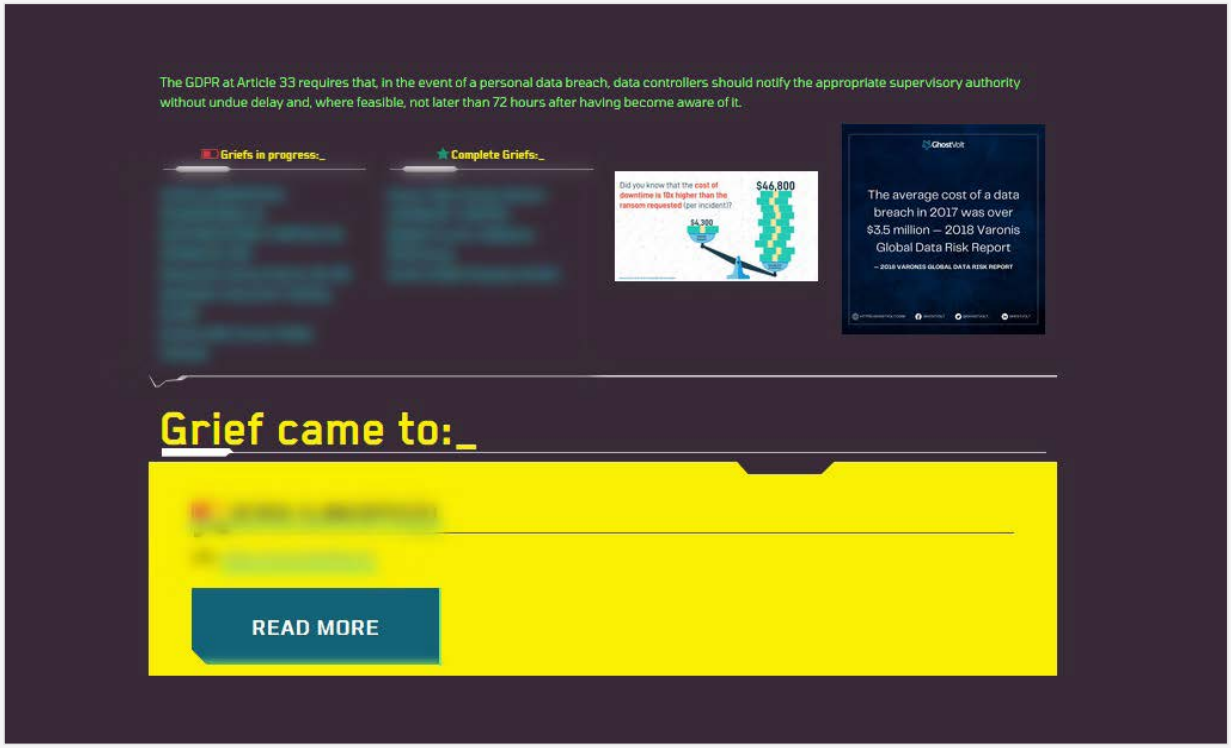

Image 3: Grief's Dark Web leak site where the ransomware gang names and shames some of their purported victims. They also flaunt statistics relating to the costs of a data breach, the cost of paying a ransom, as opposed to having a company's entire operation go down.

The Grief, DoppelPaymer, BitPaymer Connection

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."

Although the Grief Ransomware Gang (DoppelPaymer) does seem to have backed off U.S. hospitals and healthcare organisations (perhaps they do not want to capture the unwanted attention and potential serious repercussions from U.S. President Biden and U.S. law enforcement, like we saw with DarkSide and REvil/Sodin),it is clear with their current victim list, that the Grief Gang is determined to continue targeting municipalities, both in Europe and the U.S, as well as manufacturers across Europe and the U.K.

Concerned about Ransomware?

We're here to help! Submit your information and an eSentire representative will be in touch to demonstrate how eSentire Multi-Signal MDR stops threats before they impact your business.

Contact Us

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**.