eSENTIRE

EMEA THREAT RESEARCH REPORT

Notorious Russian Gang and Affiliates Increase Ransomware Attacks Against Europe

Ransomware Affiliates, Black Basta and BlackByte, Follow in Conti's Footsteps

Introduction

eSentire, a leading global cybersecurity solutions provider, has been tracking **ransomware** threats since 2019. One of the most notorious and longest-running ransomware groups is Conti. eSentire's security research team, the Threat Response Unit (TRU), has been keeping close tabs on **Conti's** illicit activities for several years. It was not until late May of this year, that the Conti leaders shut down operations as a formal entity. Although Conti "appeared to close up shop voluntarily," this was certainly not the last time critical infrastructure organisations and industry at large would hear from Conti.

In this report eSentire's research team, the **Threat Response Unit (TRU)**, focuses on two Conti affiliate groups, BlackByte and Black Basta. The two criminal gangs emerged on the ransomware scene between July 2021 and April 2022, and both of them quickly made headlines.

Between the end of February 2022 and mid-July 2022, TRU tracked 81 victim organisations listed on the BlackByte and Black Basta data leak sites. TRU has never known ransomware groups to falsely claim having compromised an organisation. Thus, they believe that the victims named on the leak sites have indeed suffered an intrusion.

Forty-one percent of the 81 organisations Black Basta and BlackByte claim as victims are based in Europe, and the other 59% are primarily located in the U.S. The U.S.-based victims include every type of business, from a manufacturer of agricultural machinery to a small regional grocery chain to several construction firms.

However, what stands out is that the U.S. companies that were attacked by these two ransomware gangs during this time frame, for the most part, are not part of critical infrastructure sectors. And yet, the European-based victim organisations are definitely **in critical infrastructure segments** including transportation, energy, government facilities, pharmaceuticals, food and education.

Within this report, TRU outlines several of the ransomware attacks, illustrating the damage that the Conti affiliates – Black Basta and BlackByte have caused and will continue to cause unless they are shut down. eSentire's experts also provide recommendations on how security leaders can prevent their organisations from falling victim to threat disruption at the hands of these malicious threat actors.

In The News: Black Basta Group

Black Basta attacks global wind turbine services company, Deutsche Windtechnik

On April 22, 2022, **Deutsche Windtechnik** – a leading global provider of maintenance services for wind turbine technologies – reported being hit by a cyberattack sometime between April 11 and 12. The attack was also confirmed by the Black Basta ransomware group when they listed the company on their data leak site (Figure 1).

Deutsche Windtechnik stated in a company **press release** that they stopped doing any "remote data monitoring" of their customers' wind turbines for one to two days, due to security reasons. However, they reported that their "operational maintenance activities for their clients resumed again on April 14, although they were running with some minor restrictions." The company called the incident a "targeted, professional cyber attack."

In response to the attack, Deutsche Windtechnik said they would be improving their IT security protections. "We are expanding our systems with higher security requirements in all units and areas.... In addition, a range of systems have been configured with even more redundance and will receive additional security support from external experts."

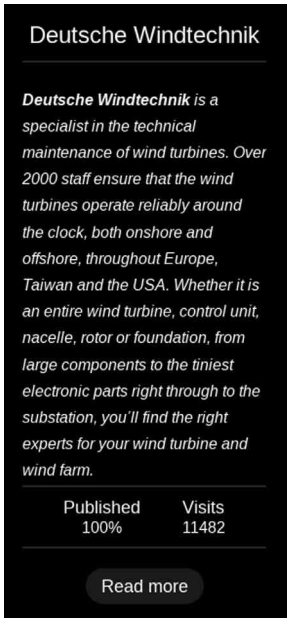

Figure 1 - Screenshot of the Deutsche Windtechnik posting on the Black Basta ransomware 'name and shame' site.

Switzerland-based national food company hit by Black Basta

On May 1, 2022, news surfaced that **The Groupe Laiteries Réunies**, a large national Swiss food company, was hit by hackers. Headquartered in Geneva, the company manages several subsidiary companies that work in the field of dairy and meat. They conduct business with over 90 local dairy and agricultural companies. The Black Basta group took credit for the attack, posting the company's name on their data leak site (Figure 2).

A Swiss news outlet also reported, "according to our information, the food cooperative was robbed of more than 140 gigabytes of documents, some of which were very sensitive on the price paid to producers and on the prices negotiated with sellers." It is not known if the food producer paid a ransom or not.

279photo Studio/Shutterstock.com

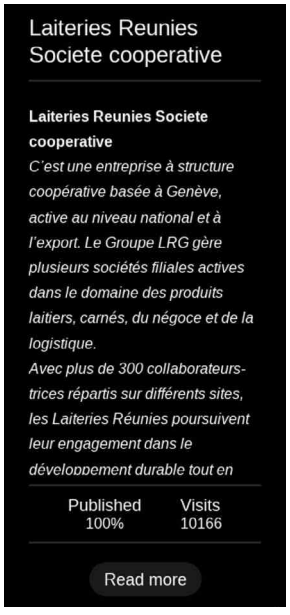

Figure 2 - Screenshot of the Laiteries Réunies posting on the Black Basta ransomware 'name and shame' site.

Black Basta shuts down a busy railway's IT systems and threatens to publish sensitive employee data and company information

On June 24, 2022, another critical infrastructure organisation in the EU fell victim to Conti affiliate, Black Basta. It was Danish railroad company **Lokaltog A/S**. The company operates six local railways on Zealand, the largest and most populated island in Denmark. Lokaltog provides transportation for almost 2.5 million residents of Zealand. According to company executives, the systems that control train operations were never disrupted because they are isolated from the company's other IT systems. However, Lokaltog's administrative systems were knocked out of commission. Luckily, the company had backups, and as a result, the company reported that their systems were back up and running on the same day of the attack.

Lokaltog also stated that they did not respond to any communications from the Black Basta cybercriminals. However, this was not the last time Lokaltog would hear from the threat actors. The Black Basta gang threatened to publish the data they had stolen if Lokaltog did not pay the money they demanded. It was blackmail at its finest. Lokaltog did not pay up, and Black Basta did as they had threatened.

They **published** the salary details of each of Lokaltog's 470 employees on their leak site. Black Basta also stole and published information about the company's board of directors, technical data about the testing of their trainsets and details pertaining to accidents on the tracks.

Lokaltog said they do not know how Black Basta broke into their IT network. And although they did have current and reliable backups, the company admitted that this attack was actually the second time, in just over a year, that they had been hit by ransomware. Lokaltog's director, Lars Wrist-Elkjær, stated: "Lokaltog is continuously taking steps to ensure that Lokaltog constantly minimises this risk of data leakage. We have also done so following this attack. The threat of hacking is constantly evolving, and it is in the wrong direction. Therefore, as a company, we must constantly follow this development."

alice-photo/Shutterstock.com

Figure 3 - Screenshot of the RadiciGroup posting on the Black Basta ransomware 'name and shame' site.

International chemical manufacturer attacked by Black Basta

In early June 2022, Black Basta announced on their leak site that they infected international chemical manufacturer **RadiciGroup** with ransomware (Figure 3). Headquartered in Italy, RadiciGroup's different businesses operate worldwide and are focused on: Specialty Chemicals, High Performance Polymers, Advanced Textile Solutions, and their products are exported all over the world.

Black Basta paralyses a large waste disposal company's phone and email systems

In or around May 24,2022, the Black Basta ransomware group attacked the IT infrastructure of Jacob Becker, a large German waste disposal company. The attack "completely paralysed" the **company's** telephone and mail system, and it also took down the company's website, according to news reports. Jacob Becker Managing Director, Thomas Pfaff, stated that the organisation was able to work in emergency mode and that garbage collection was not affected by the attack. However, they were forced to rebuild their IT infrastructure. Consequently, this took multiple weeks because they had to physically check 300 servers and 700 PCs.

Photo smile/Shutterstock.com

In The News: BlackByte Group

Conti ransomware affiliate, BlackByte, attacks transportation, healthcare, food and pharmaceutical companies in Europe

Not to be outdone by Black Basta, Conti affiliate BlackByte, whose origins go back to July 2021, also attacked its fair share of critical infrastructure organisations in Europe between February and mid-July of this year. They went after a Switzerland-based international transportation and logistics company in April of this year. Founded in 1928, the company is called M+R Spedag Group. It has 72 branch offices and 2,000 employees.

According to a May 4 **news article** in Aviation Analysis, executives with the company discovered the attack on April 21 and reported the next morning that their IT infrastructure was "fully working again." However, the company did not come out of the attack unscathed, not knowing exactly how much data was stolen or how initial access was realised.

BlackByte quickly listed the M+ R Spedag Group as a victim on their leak site and went one step further, posting 8GB of the company's date on the site as well, so anyone using the TOR anonymity network could rifle through it. The stolen documents were said to contain new and old files, including internal company data, presentations and information relating to many of the company's commercial customers. In the same May 4 article, a public relations representative for the company stated that the company's customers and partners were informed, and the company "considered the potential harm to be low." Not knowing exactly how much corporate and customer data was stolen by BlackByte, one wonders just how low the "potential harm" from this ransomware attack ended up being.

The attack against the M+R Spedag Group was far from the first critical infrastructure organisation that the BlackByte ransomware gang compromised. In fact, BlackByte had such a reputation for attacking critical infrastructure that on February 11, 2022, the U.S. Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USS) issued a joint **advisory**, warning the public that BlackByte had already attacked at least three U.S. critical infrastructure sectors (government facilities, financial, and food and agriculture) as of November 2021.

Since that time, BlackByte has continued targeting critical infrastructure organisations in Europe, and just a few in the U.S. Between February and mid-July 2022, the BlackByte gang attacked a major Italian wholesale food distributor, a pharmaceutical distributor out of Greece, and a healthcare products manufacturer out of Columbia.

Chokchai Poomichaiya/Shutterstock.com

Amongst the U.S.-based critical infrastructure organisations that BlackByte compromised between February and mid-July 2022, there were two healthcare organisations which fell victim to BlackByte. One of them was Lamoille Health Partners and is located in Northeastern U.S. The attack occurred on June 13. According to **Lamoille Health Partners**' CEO Stuart May, because of the attack, the organisation had to shut down its computer systems for a week and a half. This forced the health center's offices to close for several days so that their doctors, nurses and other employees had time to switch over to manual, paper-based processes until their computer technology could be brought back online.

In a June 30 news article, May said that they did not know if any of their data had been breached, and they were waiting for the results of the forensic investigation. "At this point, we're still going through to confirm if and what data may have been breached. Once we are able to determine, particularly relating to our patients, if there has been any unauthorised access, we'll promptly notify them in accordance with state, maybe even federal laws." At the time of publication, May did not state publicly what type of cyberattack his company had suffered. However, the BlackByte gang named them on their on their leak site, at approximately the same time that they suffered their cyberattack.

In addition to attacking Lamoille Health Partners, BlackByte's victims also include a drug rehabilitation centre, an IT services management company, a transportation company, a parts manufacturer and a supplier of components to military organisations, aerospace companies, and auto manufacturers; a telecommunications company; a community college and an array of other businesses.

BlackByte tackles the National Football League's San Francisco 49ers, and scores big

Before attacking the companies previously listed, the BlackByte gang made **news headlines** across the U.S. early in 2022. On February 12, they posted on their leak site that they had compromised the IT network of the San Francisco 49ers, one of the most popular teams in the U.S. National Football League (NFL). To convince the 49ers and others that they had succeeded in their attack, the BlackByte operators immediately began leaking files that allegedly belonged to the football team. The document archive they shared on their leak site was said to contain 292 MB worth of files, including invoices from the football organisation (Figure 4).

Spokespersons for the San Francisco 49ers did confirm on February 13 that they had suffered a cyberattack, but they did not say whether the hackers had been successful in deploying ransomware. However, a statement made by the organisation gives some indication that ransomware was deployed by the threat actors: "The San Francisco 49ers recently became aware of a network security incident that resulted in temporary disruption to certain systems on our corporate IT network. Upon learning of the incident, we immediately initiated an investigation and took steps to contain the incident....As the investigation continues, we are working diligently to restore involved systems as quickly and as safely as possible."

Figure 4 - Notification, by the BlackByte Ransomware Group on their Blog leak Site that they had compromised the IT network of U.S. pro football team, the San Francisco 49ers, and had stolen data and were providing samples of the information for free.

Unfortunately on September 2, 2022, **news** began to emerge that the BlackByte hackers did more than steal company invoices from the 49ers during their February attack. In early September, the team's management began notifying almost 21,000 people that their personal information (including names and Social Security numbers) had been accessed and potentially stolen by the BlackByte threat actors.

Conti's Sordid History

Many security researchers believe the original Conti group first came on the ransomware scene in 2018 under the name of Ryuk. However sometime in 2020, it is believed that the threat actors running Ryuk either split into two groups, rebranded or decided to begin using the "Conti" name. It is also interesting to note that the Conti ransomware code is extremely similar to the Ryuk code base.

The fact that the Conti affiliates, Black Basta and BlackByte, targeted critical infrastructure organisations, as well as manufacturers, does not surprise eSentire's Threat Response Unit (TRU). Conti's predecessor, the original Ryuk turned Conti Group, had a long history of attacking healthcare networks, energy companies, municipalities, emergency services, transportation companies and school systems, especially in the U.S. up until November 2021.

Conti's attacks were so prolific and damaging that on May 20, 2021, the U.S. Federal Bureau of Investigation (FBI) issued a **public alert** stating that among the 'Conti' ransomware victims, at least 16 were emergency medical services, 9-1-1 dispatch centres, law enforcement agencies and municipalities.

The Conti operators proved over and over again that they stand behind their threats. In March 2021, they attacked the Broward County School District in the U.S. and when the school district refused to pay the USD $40 million ransom, the hackers lowered their demands to USD $10 million, but the school system still refused to pay. As a result, Conti posted 26,000 files (mostly financial, dealing with payments, invoices, etc.) belonging to the school district on their leak site.

In 2019, the Conti Gang attacked three small municipalities in the U.S., and each of the incidents produced some debilitating effects. Collectively, the three U.S. municipalities paid the Conti operators just over USD $1.1 million in bitcoin. This ransom amount is small compared to the prices the Conti operators later charged in 2021 and 2022, when they were known to demand USD $25 million from a single victim.

According to **news reports**, the ransomware attack against Riviera Beach, Florida shut down the city's email and computer systems at their City Hall, the city's Port Center offices, and their 911 dispatchers were not able to enter calls into their computers. For some period of time, the attack also took down the systems that control the city's finances, water utility pump stations and testing systems. The Conti operators extracted bitcoin equivalent to USD $600,000 from the city of Riviera Beach and the city of LaPorte, Indiana paid them bitcoin equivalent to USD $130,000, while Jackson County, Georgia paid the Conti Gang bitcoin equivalent to USD $400,000.

It was in November 2021 that TRU noticed that the Conti Ransomware Group began to back off attacking critical infrastructure targets in the U.S. and turn their sights to critical infrastructure organisations and businesses, key to the supply chain, in Europe, the U.K. and Canada.

Interestingly, in September and October of 2021, U.S. law enforcement, under the direction of President Biden and his administration, turned up the heat on ransomware gangs, especially those attacking organisations, deemed part of a critical infrastructure sector. This included the takedown of the destructive and pervasive REvil/Sodin ransomware group and an alert issued on 9/22/21 from the **U.S. Cybersecurity and Infrastructure Security Agency (CISA)** warning companies and public entities about Conti and sharing some of the group's Tactics, Techniques, and Procedures (TTPs).

Between November 27, 2021, and February 27, 2022, **TRU** calculated that the Conti Gang claimed to have compromised 50+ new victims, and two-thirds of those organisations are based in Europe and the U.K. The remaining victims were in the U.S., Canada, Australia and New Zealand.

One of Conti's most disturbing attacks, which was made public when the threat actors posted it on their leak site on February 7, 2022, was the assault against international terminal operator, SEA-Invest. The Belgium-based company operates terminals in 24 seaports across Europe and Africa, handling liquid bulk (oil and gas), fruit & food, breakbulk, and dry bulk. SEA-Invest reported they had suffered a cyberattack against their IT networks on Sunday, January 30. As a result, "all 24 of the seaports they run across Europe and Africa were affected by the attack," according to an article in the **BBC**.

joyfull/Shutterstock.com

Conti shuts down its operation or do they?

The Conti operators racked up a slew of victims in Europe and the U.K. between the end of November 2021 and May 20, 2022. So, why did they decide to close their long-running and very profitable operation in May? The incident, which TRU believes was one of the main catalysts for Conti's shut down as a formal entity, occurred on February 27, 2022.

On that day, more than 60,000 internal chat logs and a host of financial documents, belonging to the **Conti Group** were leaked on the Internet. These chat logs gave security professionals an invaluable view into Conti's operations, providing rare intelligence about the threat group's tactics, techniques, and procedures (TTPs), their management structure, their IT infrastructure and much more.

A Ukrainian security researcher is suspected of leaking the sensitive data, in retaliation for one of the Conti members posting a declaration of support for Russia on their leak site, just one day after Russia's full-scale invasion into the Ukraine (Figure 5). The warning stated if anyone organised a cyberattack or any war activities against Russia, they would use "all possible resources to strike back at the critical infrastructures of an enemy."

Figure 5 - Screenshot from the Conti 'name and shame' page indicating their support for Russia, posted on February 25, 2022.

Later, on March 1, the Conti gang revised its warning message slightly, stating that the Conti gang "condemned the ongoing war, however, they would use their full capacity to retaliate if there were any attempts to target critical infrastructure in Russia or any Russian-speaking region of the the world." See Figure 6.

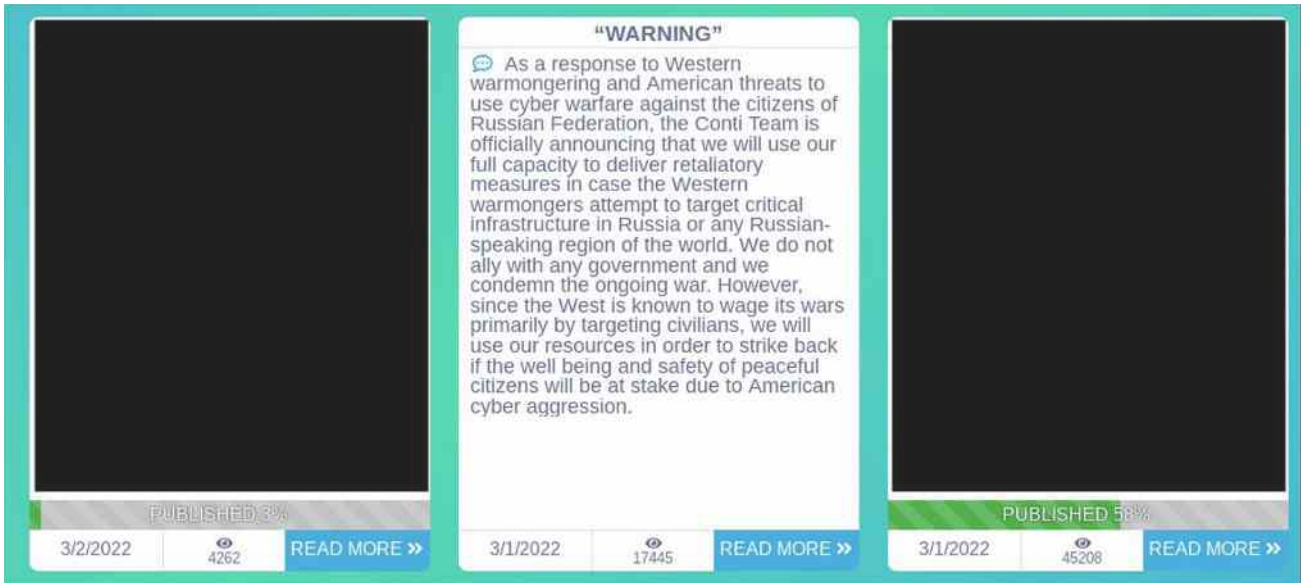

Figure 6 - Screenshot from the Conti 'name and shame' page indicating their support for Russia, posted on March 1, 2022.

After the data leak incident, the Conti operation lost steam. However, before officially "closing up shop" at the end of May, the Conti gang decided to go out with a "bang."

In April 2022, Conti launched a series of crippling attacks against the government of Costa Rica. **News reports** stated that the attacks caused damage to numerous government ministries, severely affecting the country's ability to function. For example, the attack left part of Costa Rica's digital infrastructure crippled for months, paralysing online tax collection, disrupting public healthcare and the pay of some public sector workers.

The Conti group demanded USD $10 million ransom from the Costa Rican government, which the government declined to pay. Consequently, the Conti Gang published 672GB of data belonging to the Costa Rican government agencies, on their leak site. Costa Rica declared a national emergency on May 8.

Ten days later, the Conti operators began dismantling their infrastructure and began shutting down their operation. However, TRU theorises that the top Conti operators simply joined up with already existing Conti affiliate groups, like Black Basta and BlackByte, or started new Conti affiliate groups.

As evidenced by the attacks and the damage caused by the Black Basta and BlackByte affiliates, the Conti threat is alive and well, and as destructive as it has always been.

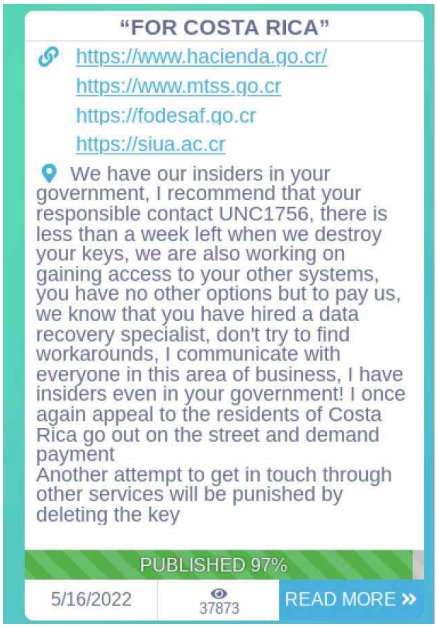

Figure 7 - Screenshot of the Costa Rica government compromise posting on the Conti 'name and shame' page.

Recommendations From TRU to Protect Your Organisation From This Cyber Threat

As the adversarial TTPs grow in sophistication, they create a level of challenge that once reached, critical business decisions must be made. Preventing the various attack paths utilised by the modern threat actor requires actively monitoring the threat landscape, developing, and deploying endpoint detection, and the ability to investigate logs and network data during active intrusions.

Initial Access

Initial Access for ransomware operations is typically achieved using valid VPN and Active Directory (AD) user credentials, which are stolen using phishing emails, infostealer malware, social engineering tactics and remote exploitation. Social engineering may occur through phishing and business email compromise (BEC) attempts and SEO poisoning. Remote exploitation occurs on the organisation's Internet-facing systems when those systems are vulnerable. To increase your cyber resilience against Initial Access attempts, we recommend:

- **Endpoint Monitoring:** Deploy an **Endpoint Detection and Response solution** for 24/7 endpoint monitoring to workstations, ensure the endpoints leverage rules around User Execution and Windows Proxy Execution.
- **Cybersecurity Awareness Training:** Ensure your employees understand the dangers of phishing emails and business email compromise (BEC) attacks and malicious web browser downloads through **Phishing and Security Awareness Training (PSAT)**. Your IT cybersecurity team should have a reporting process in place that does not punish users in case they accidentally click on a malicious link as punishing users discourages reporting.
- **Email Filtering Appliances:** Email filtering appliances can detect and stop spam mail.
- **Network Monitoring:** Automatically block known malicious infrastructure and investigate suspicious packet behaviour using a **Network Detection and Response** solution to help disrupt cyberattacks before they lead to infections.
- **Vulnerability Management:** Adopt a comprehensive **vulnerability management program** so you have an updated inventory for all your assets, identify existing vulnerabilities and which ones can be exploited, and prioritise them based on the threat landscape. Different vulnerabilities have a different probability of being exploited with varying degrees of consequences. Knowing the types of vulnerabilities and the state of exploit maturity among threat actors can help prioritise patch management. In addition, you must consider misconfigurations since misconfiguring an Internet-facing device can sometimes have the same consequences of a vulnerability.

Lateral Movement

It's important to understand that you can't assume that every Initial Access vector can be stopped. Given sufficient time and size of organisation, some fraction of employees will inevitably download and execute malware and give their credentials to phishing campaigns, resulting in threat actors gaining access and moving laterally across your environment. Some administrators will miss a patch or misconfiguration because there can be many patches to prioritise at different times in the year as the cybercrime seasons change. Therefore, we recommend:

- **Endpoint Monitoring:** Ensure endpoint coverage is extended to domain controllers, email servers, and other internal systems with increased privileges where threat actors will attempt to pivot to. Ensure some endpoint monitoring around administrative commands pertaining to credential access, environment discovery, and lateral movement.
- **Log Monitoring:** Ensure **security logs** are collected for workstations, servers, and domain controllers. Hands-on ransomware intruders will sometimes register their own VM in the VPN pool. These attackers become hard to trace without AD log files. Logs from privileged network appliances, like IIS, Citrix, and Exchange can sometimes be the only source of telemetry for how those appliances are abused by active intruders.

Impact

Impact happens when the ransomware operation is successful. There are various levels and markers of success, from exfiltration to disrupting business directly through ransomware. Therefore, we recommend:

- **Endpoint Monitoring:** Ensure there are endpoint rules around finding and deleting backups, credential access, and exfiltration.
- **Network Monitoring:** Flow data can help investigate details about exfiltration, such as how much data was sent or received between hostile IPs and assets.
- **Tactical:** Defenders are engaged to intercept hands-on attackers and kick them out before they can disrupt business. If required, eSentire's Incident Response team can be engaged. In cases where exfiltration or other high impact actions are suspected, eSentire's Incident Response team is engaged.
- **Incident Response:** Be ready to engage a **Digital Forensics and Incident Response** provider so you can gain peace of mind knowing that you're prepared for even the most advanced cyberattack.

How the eSentire Threat Response Unit (TRU) Responds to Ransomware Groups

eSentire's Threat Response Unit (TRU) is a world-class team of threat researchers who proactively hunt advanced, undetected threats as a means of continuously improving eSentire's Managed Detection and Response (MDR) expertise to help our global customer base stay ahead of attackers. TRU combines threat intelligence obtained from research and security incidents to create practical security outcomes that provide immense value:

Tactical Response

Defenders are engaged to intercept hands-on attackers and remove them from the environment before they can disrupt business operations.

Operational Response

The adversarial infrastructure, tactics, and other artifacts tracked by TRU are continuously swept through indicator hunts and rule deployment and our team of **24/7 Cyber SOC Analysts** actively monitors these signals for disruptive attacks.

Strategic Response

TRU continues to build out its threat actor tracking capabilities as the threat landscape shifts. Deploying new threat detections and intelligence products to the SOC, and the cybersecurity community at large, are an ongoing endeavor.

Our detection content is supported by investigation runbooks, ensuring our SOC (Security Operations Centre) analysts respond rapidly to any intrusion attempts related to known malware TTPs. In addition, TRU closely monitors the threat landscape and constantly addresses capability gaps and conducts retroactive threat hunts to assess customer impact.

eSentire's Threat Response Unit (TRU) is a world-class team of threat researchers who develop new detections enriched by original threat intelligence and leverage new machine learning models that correlate multi-signal data and automate rapid response to advanced threats.

If you are not currently engaged with an MDR provider, **eSentire MDR** can help you reclaim the advantage and put your business ahead of disruption.

Ready to Get Started?

Learn what it means to have an elite team of Threat Hunters and Researchers working for you, as an extension of your team. Connect with an eSentire Security Specialist.

Contact Us

If you're experiencing a security incident or breach, contact us (0)8000 443242

eSentire