SHADOWBYTE

CASE STUDY:

SOCIAL MEDIA

How ARIA helped a social media giant identify stolen account vendors and take down leaked databases containing sensitive customer information.

THE CUSTOMER

As one of the largest social media companies on the planet, this company has over a billion active users, and employs tens of thousands of people globally, and in 2020, earned roughly $86 billion in annual revenue.

THE PROBLEM

The market for buying and purchasing stolen accounts and databases is enormous. There is also a major market for the buying and purchasing of hacked or stolen social media accounts. Hackers are able to generate tens of thousands of dollars in revenue per week by selling access to hacked social media accounts, which they often advertise the sale of on the very platform whose customers they hacked.

In addition, unsecured public databases often leak sensitive data information, usually containing identifiable social media information. In many cases, data leaked through unsecured public databases is done so illegally via data scraping. In order to crack down on sites illegally collecting data on its users, this company needed a way to monitor public databases containing identifiable customer data in order to send the appropriate legal takedown notices.

THE SOLUTION

In February 2021, many news outlets reported a coordinated takedown between several social media companies targeting account thieves”.

KEY TAKEAWAYS

- ARIA platform used to monitor public databases containing illegally obtained or leaked customer user data in order to send appropriate legal takedown notices.
- Leverage ARIA’s search and watchlist features to identify stolen account shops and vendors.
- Information obtained used in publicly announced sting operation to takedown known vendors and their stolen account shops.
- Proprietary technology crawls and indexes publicly leaked databases to to identify illegally obtained content.

Several of ARIA’s key modules provided the critical intelligence needed to facilitate this. Stolen account shops, sellers, and resellers can be easily targeted and researched using ARIA’s advanced forums, marketplaces searches, and watchlist features.

The targeting and coordinated takedown of servers leaking sensitive data customer information was facilitated using ARIA’s ‘meta-search module, which crawls and tags metadata from public databases. Any data matching specific parameters were sent to internal incident response teams in order to begin the process of legally taking down any server or service illegally obtaining customer data.

SHADOWBYTE

CASE STUDY:

HOTEL AND CASINO

Counterintelligence team tasked with establishing communication with a cyber threat actor to acquire potentially stolen data detected by ARIA.

THE CUSTOMER

As one of the world's most recognizable casino and hotel brands, this customer is an icon of American global hospitality and entertainment, operating more than thirty world-class hotels and casinos globally.

THE PROBLEM

A threat actor associated with a well-known cyber-terrorist hacking group began offering the sale of data allegedly stolen from the customer. The actor in question was a known member (or associate) of The Dark Overlord group, which has claimed responsibility for a number of other high-profile hacks and intrusions.

This scenario was especially troubling because the data was being offered by someone with an established reputation for hacking and selling high-profile databases.

News or mentions of this particular threat actor were flagged by Shadowbyte ARIA application, which generates real-time alerts for our threat hunting team. Within several hours of its original posting, Vinny Troia, Shadowbyte's CEO, contacted the customer's chief information security officer (CISO), alerting him of the active sale. Shadowbyte was then retained to establish communication with the actor in order to validate the data and learn how it was obtained.

THE SOLUTION

At the behest of the customer's security team, Shadowbyte's counterintelligence unit established direct communication with the hacker.

KEY TAKEAWAYS

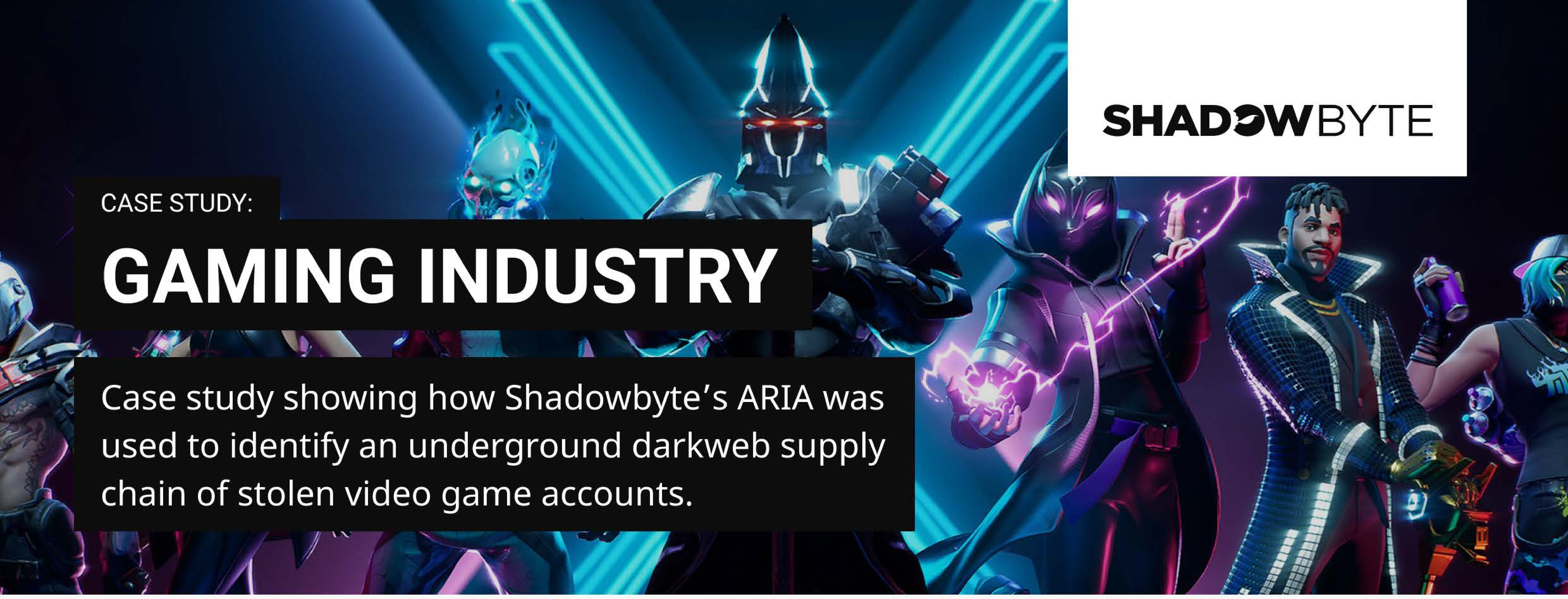
- Shadowbyte's counterintelligence team discovered an actor of a known cyber-terrorist hacking group selling allegedly breached data on a dark web forum. data on the darknet.
- Our team notified the organization in question and was subsequently hired to establish communication with the threat actor.
- Our threat intelligence analyst was able to establish a rapport with the actor in order to elicit information on how the breach occurred, allowing the customer to remediate the vulnerability.

In direct conversations, our analyst posed as an interested buyer of the data. After several lengthy discussions, a rapport was established with the actor, at which time he began to brag about his accomplishments.

After our analyst was able to apply social engineering techniques to elicit the criminal into providing details on the breach was carried out. The actor also shared a copy of the data with our team, which was then sent back to the client for direct analysis and validation.

Our team worked directly with federal law enforcement agents to provide critical information on the actor, which included his current and past-aliases.

The information provided to the customer was validated and used to close the previously exploited vulnerability.



CASE STUDY:

GAMING INDUSTRY

Case study showing how Shadowbyte's ARIA was used to identify an underground darkweb supply chain of stolen video game accounts.

THE PROBLEM

Epic Games, Inc. is a leading video game development company based in the United States.
With Fortnite's immense popularity, the game has become a lucrative target for cybercriminals.
The value of a hacked Fortnite account comes from the character's in-game "skin".

These Fortnite accounts are initially hacked via simple credential stuffing techniques using username-and-password combinations extracted from data. Those "combos" are then checked against Epic Games' servers to look for valid Fortnite accounts. This method of finding valid Fornite accounts is extremely easy as many people fall into the trap of re-using their passwords.

MILLIONS OF DOLLARS OF BLACK MARKET REVENUE

Shadowbyte's dark web intelligence teams noticed a huge surge in the procurement and sale of these stolen Fortnite accounts, prompting us to begin our research. As we began to unravel the details of this underground cybercrime economy, we reached out to Epic Games' security and legal teams to discuss our findings and offer our assistance. Unfortunately, Epic was unwilling to even have a conversation with us, claiming they had the situation under control.

As our research continued, it became clear that high-profile Fortnite vendors were clearing tens of thousands of password variations in a short amount of time, essentially causing a complete shutdown of stolen Fortnite account sales.

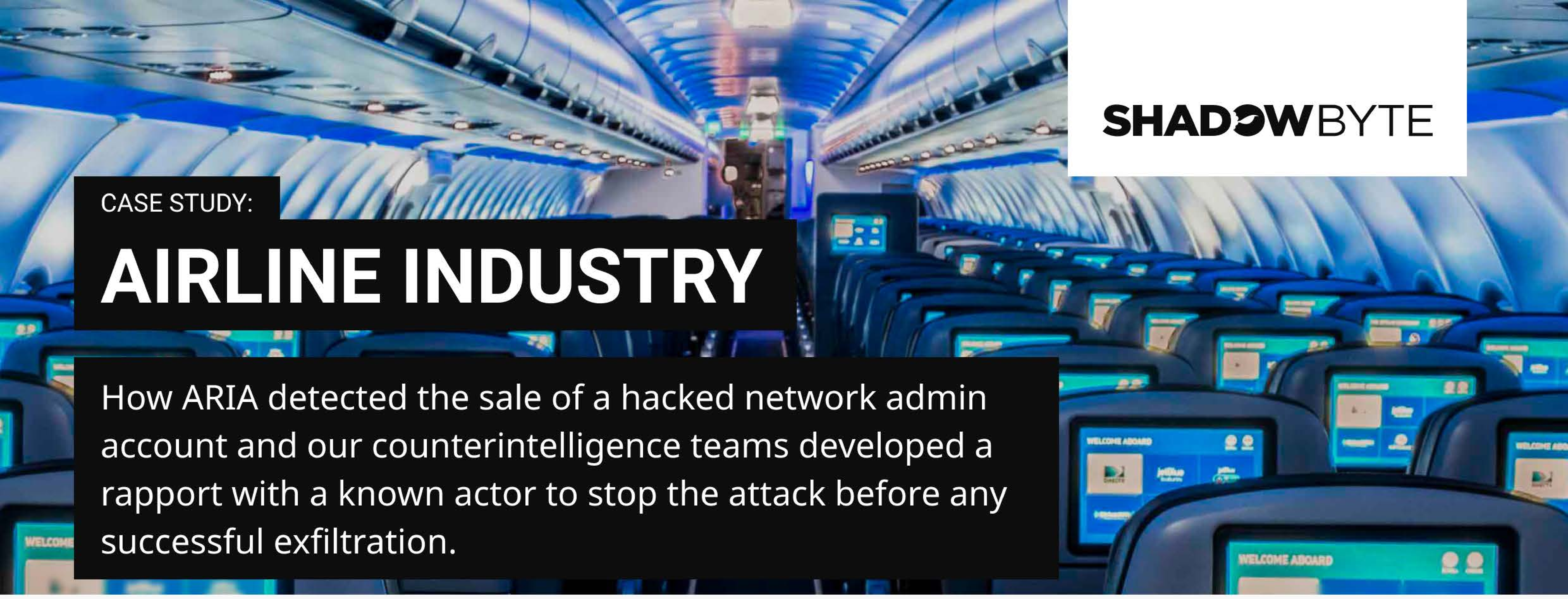
KEY TAKEAWAYS

- Shadowbyte's prompt research and investigation shed light on the highly profitable hacked-account underground account market within the gaming community.
- Following the publishing of Shadowbyte's report, Fortnite implemented a CAPTCHA challenge with each login request, slowing down the credential stuffing attacks to a crawl.
- Hackers could no longer test tens of thousands of password variations in a short amount of time, essentially causing a massive shutdown of stolen Fortnite account sales.

FORCING SECURITY THROUGH PUBLIC AWARENESS

Shadowbyte's report on "The Fortnite Underground Cybercrime Economy", added significant awareness to the ongoing gaming account black market, forcing Epic Games to finally get involved. Following the media coverage generated by our report, Epic implemented a CAPTCHA challenge with each login request, slowing down the credential stuffing attacks to a crawl.
This meant that hackers could no longer test tens of thousands of password variations in a short amount of time, essentially causing a complete shutdown of stolen Fortnite account sales.

This slowdown virtually eliminated Fortnite fraud for four months before hackers found a way to bypass new login methods.



SHADOWBYTE

CASE STUDY:

AIRLINE INDUSTRY

How ARIA detected the sale of a hacked network admin account and our counterintelligence teams developed a rapport with a known actor to stop the attack before any successful exfiltration.

As one of the world's most recognizable airlines, this airline operates more than one thousand flights daily. They are ranked in the top 10 airlines, globally, and were named one of the best companies to work for by Forbes.

Because it employs so many people and flies so many passengers on an annual basis, protecting the privacy of its customers is always a top priority. This airline's massive global footprint of data, infrastructure, employees, passengers, and digital assets makes it a frequent target of cyberattacks.

THE PROBLEM

Shadowbyte's threat intelligence team became aware of a threat actor selling admin access to their internal infrastructure and was actively attempting to exfiltrate data from the organization.

A threat actor had successfully gained admin access to the Airline's Office365 account, resulting from the admin re-using passwords across multiple services. The hacker was able to use the administrator account to pivot to other locations within their Azure environment. Access to those systems was being sold in very private circles. The sale of this access or exfiltration of any private data would have caused a catastrophic situation for the organization, especially if it fell into the hands of a nation-state or terrorist organization.

KEY TAKEAWAYS

- Using ARIA, Shadowbyte identified an actor selling admin access into a major airline's network.
- The actor gained access to the admin account using a common or re-used password.
- Our counterintelligence team developed a rapport with the actor in order to elicit the information to locate them within the network.
- Using the information provided, the Airline was disable any hacked accounts and stop data exfiltration attempts.

THE SOLUTION

After establishing the threat and sale as credible, Shadowbyte's CEO, Dr. Vinny Troia, immediately contacted the head of the airline's cybersecurity team to brief them on the emerging situation. Even with this information, the actor was able to evade detection by their security teams.

Dr. Troia continued to build rapport with the hacker. Once trust with the threat actor had been established, Troia was able to persuade the attacker to run a series of commands within the infrastructure as proof of his network access. Those specific commands allowed the airline to isolate the rogue admin account and completely lock the actor out of the network.

SHADOWBYTE

CASE STUDY:

LAW ENFORCEMENT AGENCY

Tracking & identifying The Dark Overlord cyber hacking group using Shadowbyte's ARIA platform.

BACKGROUND

A cyber terrorist hacking group known as the 'Dark Overlord' became notorious in 2016 for extorting and terrorizing organizations across the country. Their specialty was extorting medical and healthcare providers and they became famous in the media for selling stolen medical records on the darknet markets. In addition to medical facilities, they also liked to extort law firms and successfully hacked a number of them in Missouri. The Dark Overlord group really hit the big time in 2017 when they began to extort household brands like Disney, Netflix, ABC, and Fox after hacking them and threatening to publish previously unreleased copies of their studio productions on the internet if their ransoms were not paid. They were the group behind the illegal release of the Netflix series 'Orange Is The New Black' after Netflix point blank refused to pay their ransom or give in to the criminal group's extortion attempts.

They went on to become known as terrorists when they began to hack entire school districts and threaten the safety of their student bodies unless their ransoms were not paid, forcing more than 30 schools to close for weeks while the attacks were remediated by cybersecurity professionals. After hacking school records the group would begin to send text messages to the children's families, naming them personally in the messages, and making threats of violence against them, often threatening to kill the children. Even more maliciously they began to publish the phone numbers and names of children online and encouraged pedophiles to target them.

KEY TAKEAWAYS

- Night Lion security conducted an exhaustive two-year intelligence-gathering campaign on the notorious cyber-terrorist group and published a report of key evidence against them.
- The Night Lion report identified two of the leading members behind the Dark Overlord cyber-terrorist group and worked with their local FBI contact to plan their campaign.
- As a result of Night Lion's intelligence report, members of the Dark Overlord cyber-terrorist group were identified and eventually apprehended, bringing their reign of terror to an end.

HOW WE HELPED

Vinny Troia and the team at Night Lion Security had been actively tracking the cybercrime group for a number of years and gathering intelligence on the group in order to provide evidence to law enforcement officials. Members of Nigh Lion's Intelligence Division began formulating a plan to penetrate the group and gather as much identifying information as possible, during the planning phase they worked closely with their local FBI contact.

Night Lion Security published an intelligence report which helped to identify the head of Dark Overlord as a nineteen year old Canadian called Christoper Meunier and his long time collaborator, Canadian citizen Dennis Dionysios Karvouniaris. This report was instrumental in the Dark Overlord crime group being apprehended and brought to trial, it also provided evidence of a close and long-term collaboration between these two perpetrators and their history operating under different names on various darknet forums and markets. The report directly attributed the close collaboration between these two figures with approximately 42% of (non-credit card related) data breaches between 2017 and 2020 and provided evidence of the two hacking Night Lion servers in an attempt to discredit its findings.

The intelligence report published by Night Lion was instrumental in helping federal law enforcement officials identify and extradite key members of the group in order to bring them to trial in the United States, arrests which resulted in convictions for the Dark Overlord members.