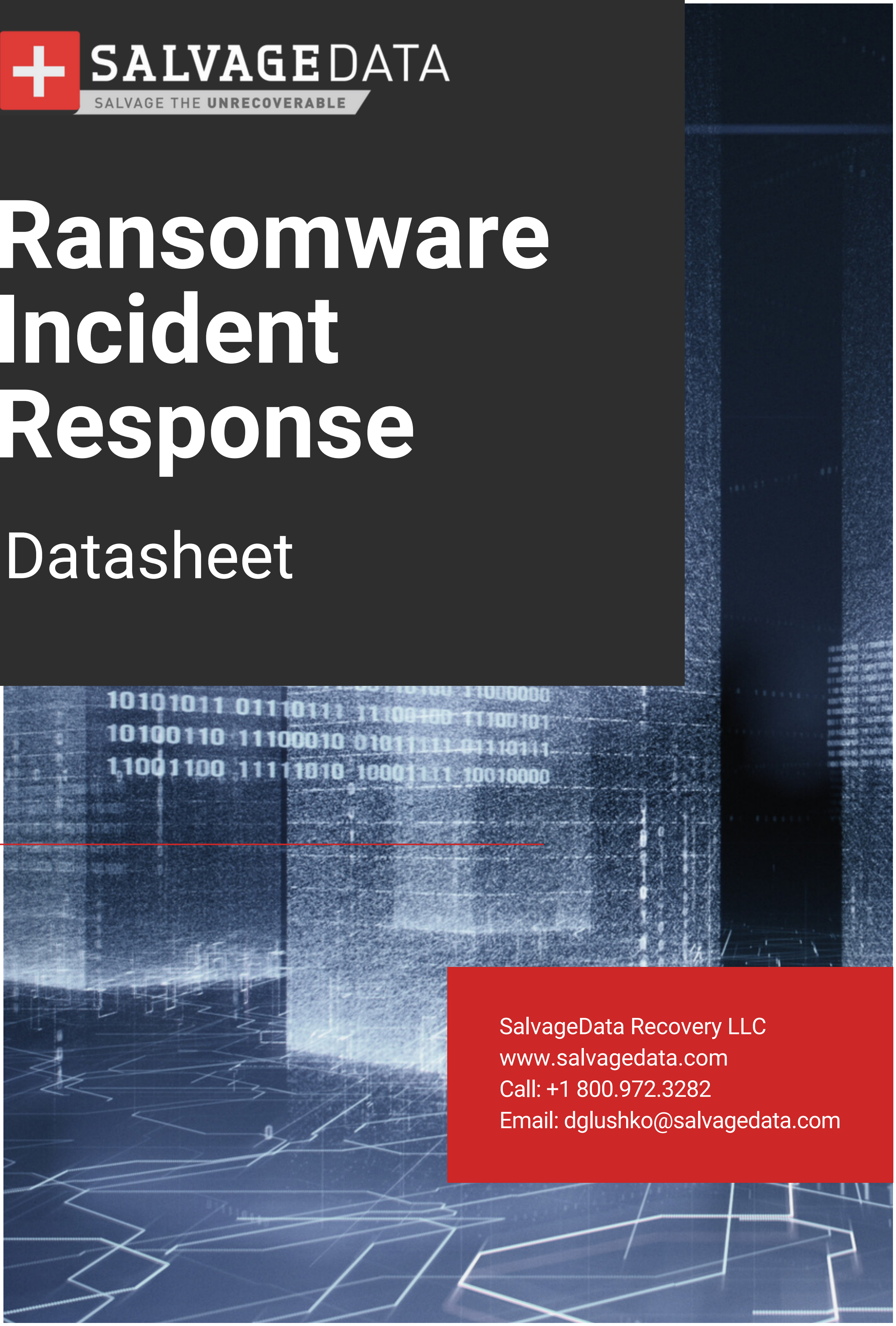
SALVAGEDATA
SALVAGE THE UNRECOVERABLE

Ransomware Incident Response

Datasheet



SalvageData Recovery LLC
www.salvagedata.com
Call: +1 800.972.3282
Email: dglushko@salvagedata.com

Datasheet

INCIDENT RESPONSE SERVICES: RANSOMWARE RECOVERY

EXECUTIVE SUMMARY

COUNT ON SALVAGEDATA TO BE YOUR COMPLETE SOLUTION FOR RANSOMWARE INCIDENT RESPONSE

Founded in 2003, SalvageData has accumulated experience in ransomware removal and encrypted data restoration. From our headquarters in Cleveland, Ohio, we have helped hundreds of clients successfully recover from ransomware attacks. Our pioneering experimentation with quantum computing combined with our own tools and technology have assisted our works in identifying attack vectors, securing environments, breaking encryption, remediating servers and workstations, and supplying organizations with forensics Breach and Infiltration reports.

Our mission is to restore normality after a ransomware attack with heavy consideration for time and money. In over 50% of our cases, our efficacy in reverse engineering the encryption as well as our Research & Development efforts, are able to remove the malware and we can avoid paying the ransom. In cases where that is impossible, especially within the Recovery Time Objective (RTO), our compliance program with FinCEN and OFAC allows us to legally negotiate a much lower ransom in exchange for a secure decryptor, which we test before any payment is made.

You can't predict when a ransomware attack will happen, but you can count on SalvageData to be at your side 24/7/365.

RANSOMWARE ATTACKS ARE INCREASING

NO BUSINESS IS SAFE FROM MALWARE THREAT ACTORS

While ransomware attacks are only one facet to consider in cybersecurity, the way it is handled can be detrimental to the future of any business. Worse still, ransomware attacks are becoming increasingly common and are considered one of the fastest-growing cybersecurity threats, with new advancements and sophisticated methods being used to spread malware.

According to research published by Cybersecurity Ventures in 2021, cyber attacks are estimated to occur every 11 seconds, and cost businesses around the world more than $20 billion.

SalvageData's incident response team continuously monitors threat actors, trends, and high-end decryptor technology - all this empowers us to strike fast and reduce damage in the three main fronts that threat actors target:

TIME

Threat actors may tend to bluff in their ransom demand, but downtime due to a ransomware attack is very real. SalvageData gets ahead of the issue by having our team of experts always ready to deploy our **emergency protocols 24/7**. Once activated, we work from multiple angles to quickly analyze and report the damage, and find the fastest malware removal opportunity.

COSTS

Our work in decryption and data carving can allow victims to avoid paying the ransom most of the time. And even if negotiating with the threat actors becomes the only option, our work gives us the leverage needed to effectively reduce the ransom amount, sometimes up to **99% less than the initial demand.**

LEGAL LIABILITY

Ransomware attacks are made to tear through privacy and security protocols, easily compromising critical and sensitive data. Our thorough forensic analysis & report have given our clients legal liability protection, and when absolutely necessary, our strict **FinCEN and OFAC compliance program** makes it possible to legally negotiate terms and the ransom payment with the threat actors.

WHY SALVAGEDATA?

REDUCE DOWNTIME, REDUCE DATA LOSS, AND REDUCE THE RANSOM. COUNT ON SALVAGEDATA'S TEAM TO RECOVER FROM A RANSOMWARE ATTACK.

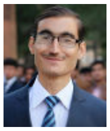
While ransomware attacks are only one facet to consider in cybersecurity, the way it is handled can be detrimental to the future of any business. Worse still, ransomware attacks are becoming increasingly common and are considered one of the fastest-growing cybersecurity threats, with new advancements and sophisticated methods being used to spread malware.

TOP WHITE-HAT HACKERS

Ransomware recovery is only possible if you know what you're dealing with. This powerful team is continuously researching the thousands of ransomware variants, new trends, and TTPs (Tactics, Techniques, and Procedures) to stay up-to-date with the Threat Landscape. By familiarizing themselves with the encryption codes they are able to find the "chinks in the armor" which is what allows SalvageData to develop decryptors in-house so that no ransom payment is needed.

Jade Thuo
Cryptologist

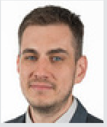
Piotr Karwowski
Malware analyst



Jawad Ali
Malware and cryptography analyst

EXPERT DATA CARVERS

Threat actors are quick to claim that critical data is fully encrypted and impossible to retrieve without paying the ransom. But while our mediation experts deal with reducing the ransom demand and testing the accuracy of their claims, our team of Data Carvers gets right to work in combing through the encryption to learn everything they can. This often means that they find out if the type of data is indeed critical or sensitive and - most importantly - if they can decrypt the data themselves.



Dmitriy Lif
Head Data Carver

AJ Wunderle
File system & file type engineer

Michael Galloway
Mobile data specialist

EFFICIENT RANSOMWARE TECHNICIANS

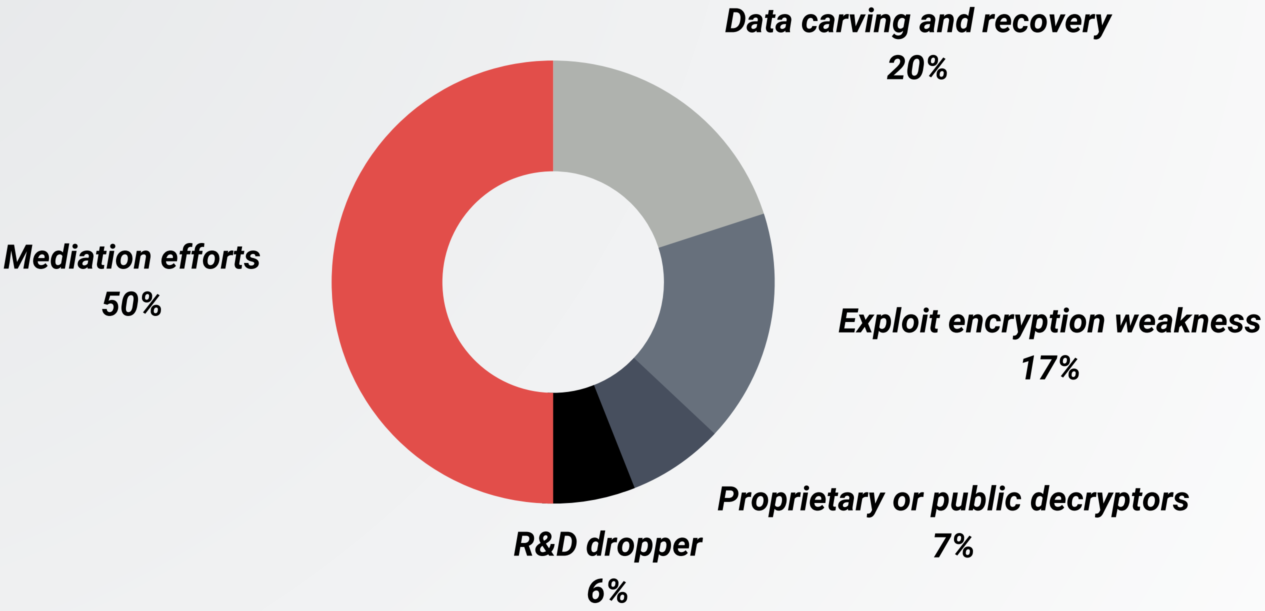
Once our in-house cryptologists have developed a custom decryptor for the particular malware, our Ransomware Technicians jump into action. Carefully testing and running the decryption key through all affected data and devices, all while ensuring that the data retrieved is not corrupted, tampered with, or leaked.

Michael Sicat
Ransomware technician

Sahir Anees
Ransomware technician

Jesus Filio
Ransomware technician

HOW SUCCESSFUL ARE RANSOMWARE REMOVAL STRATEGIES:



CONTINGENT SERVICES

Recovering quickly from a ransomware attack is no simple matter. If your clients need extra help that will work alongside their in-house team, SalvageData's experts can assist with professionalism and speed. Or, if they prefer, we are qualified and able to provide these services independently.

FORENSICS INVESTIGATORS

There are 3 main questions that any victim of a cyberattack needs answered: how the attack happened, who was responsible, and how to prevent it from happening again in the future. That's where our cyber security forensics investigators can step in, and collect and analyze data from various sources, identify the source of the attack, assess the damage caused, recommend security measures, and may testify in court if the investigation leads to legal action.

CYBER SECURITY TECHNICIANS

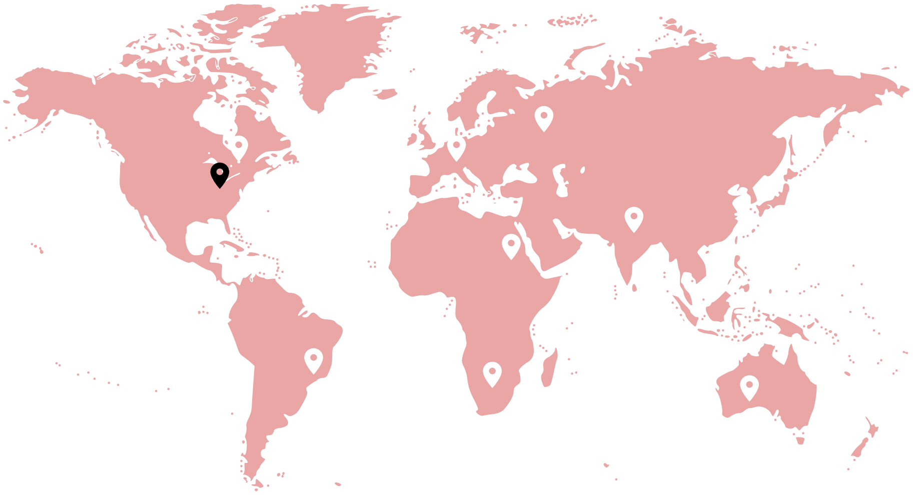
Trained for the worst-case scenarios, our Cyber Security Technicians will immediately implement security controls to prevent further damage and mitigate the ransomware from spreading. Our top priority is removing the ransomware safely and restoring access to the encrypted files. Finally, this team will conduct vulnerability assessments and risk analyses to prevent a future attack.

SYSTEM ADMINISTRATORS FOR ENVIRONMENT AND NETWORK REMEDIATION

Time cannot be wasted, and your clients need to restore their business back to normality as soon as possible. Our System Administrators for Environment and Network Remediation will work to restore the affected systems to their pre-attack state, including removing any remnants of malicious software, implementing improved security measures, patching any vulnerabilities, and restoring data from backups.

UNIQUE CAPABILITIES

While our technicians are our greatest asset, we didn’t stop there. SalvageData stands out as an incident response services provider by continuously raising the standards on what can be expected in terms of security, privacy, and support.



24/7 ASSISTANCE WORLDWIDE

Ransomware attacks can be dangerously unpredictable. You need your incident response team to be able to give immediate assistance and damage control. SalvageData offers around-the-clock services and more. This includes having a team member deployed **onsite within 24 hours** of starting a case to get started on damage control.

OVER 50% SUCCESS RATE IN AVOIDING THE RANSOM

Paying the ransom is the last resort. Take advantage of SalvageData's years of experience in malware research & development, whitehat hacking, and cryptology; without paying cybercriminals a single cent.

70% REDUCTION IN THE RANSOM DEMAND

If we get to the last resort, SalvageData has a unique compliance program with FinCEN and the OFAC which allows our experts to negotiate the ransom with the hackers. On average, we are able to reduce the ransom amount by 70-99% with our negotiation tactics.

OFAC & FINCEN COMPLIANCE

In 2020 the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) declared it illegal to pay a ransom in most cases. SalvageData's legal team has worked alongside the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) to develop a compliance program that increases the chances of ransomware recovery by allowing us to negotiate with the threat actors when paying the ransom is the only option to retrieve encrypted data.

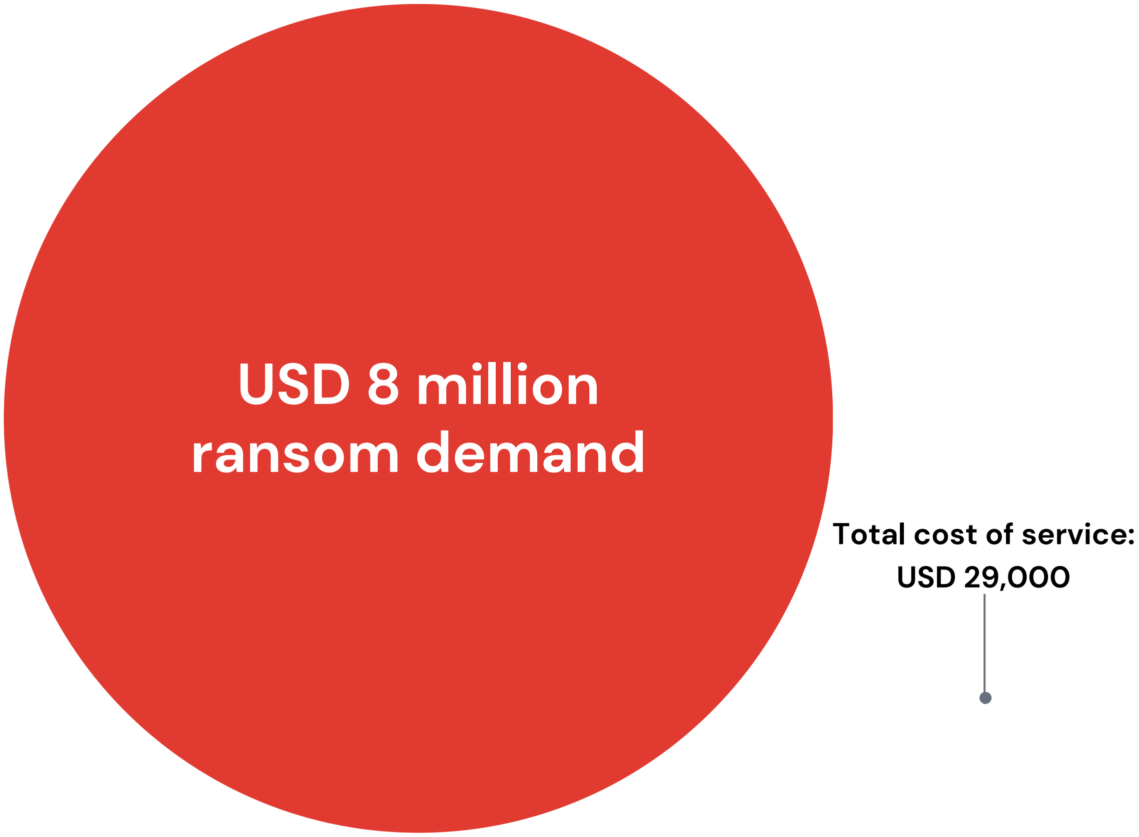
EXPERIENCE IN RANSOMWARE

SalvageData's extensive experience means that we are proficient in handling all types of ransomware variants. We understand the importance of swift action when a cyber attack occurs and our incident response services quickly identify and contain the attack, minimize damage, and recover lost data. Additionally, SalvageData keeps up-to-date on the latest developments and trends in ransomware variants, which allows us to provide the best possible service and safeguard against future attacks.

CASE STUDY: ROYAL VARIANT

- Industry: Data center and cloud computing
- Number of employees: 5,000
- Type of data encrypted: SQL Database / Virtual Machines
- **USD 8 million ransom demand**

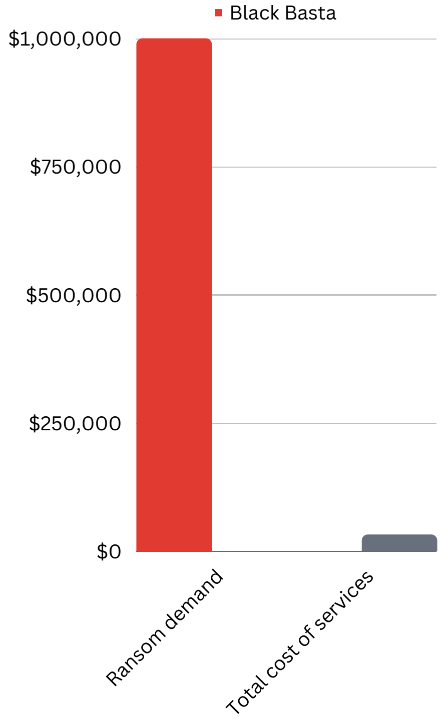
- Inhouse decryption - no payment to threat actors
- Forensic report provided
- Shell script provided
- Total time for full recovery: 5 days
- **Total cost of service: USD 29,000**

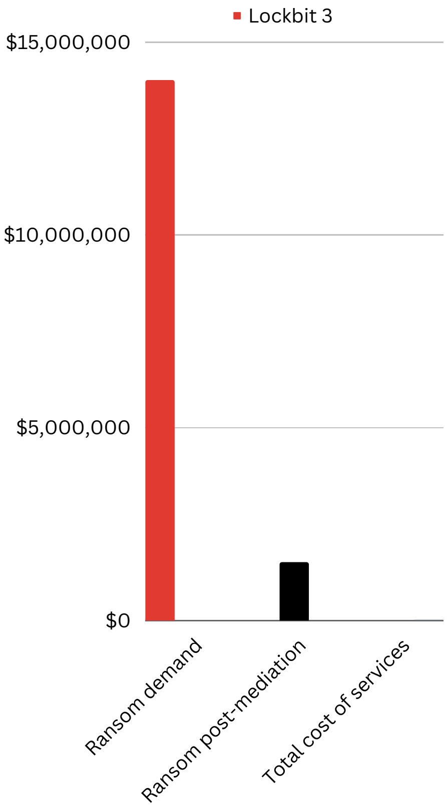


CASE STUDY: BLACK BASTA

- Number of employees: 200
- Industry: Legal
- Type of data encrypted: Virtual machines & file shares
- **USD 1 Million ransom demand**

- The forensics investigation report concluded the threat actors' allegations of exfiltrated data were false.
- Inhouse decryption was able to recover most of the data by exploiting a weakness in the encryption
- Repaired the corrupt data
- Total time for full recovery: 2 weeks
- **Total cost of services: USD 32,000**





CASE STUDY: LOCKBIT 3

- Number of employees: 6,500
- Industry: Science and Technology
- Type of data encrypted: VMware Esxi hosts
- **USD 14 Million ransom demand**

- Worked alongside the client's cybersecurity consultants
- Negotiations reduced the ransom demand to USD 1.5 Million
- Assisted in securing cryptocurrency under the compliance program
- Total time for full recovery: 48 hours
- **Total cost of services: USD 5,900**

SERVICE HOURS

You can reach one of our data recovery consultants between 9AM and 5PM (Eastern Time) Monday through Friday at 1.800.972.DATA(3282). Or e-mail **support@salvagedata.com.**

EMERGENCY ASSISTANCE

For emergency/weekend/holiday assistance, call 1.800.972.DATA(3282) and an on-call data recovery consultant will help you.

SERVICE LEVELS:

STANDARD SERVICES

Usually requested when the ransomware is a private problem and can be resolved by our technicians. This includes: running decryptors, file repair tools, using public solutions, etc.

EXPERT SERVICES

Is necessary for more dangerous cyber attacks that may be fully or partially considered a public concern. This requires the attention of our engineers and will usually include: any type of forensics, cybersecurity, reverse engineering, cryptography work, etc.

MEDIATION SERVICES

Last resort service, but important to consider it in advance, so as to not waste precious time. Our reputation as a ransomware removal service provider, and our expertise in decrypting so many known ransomware variants, are what makes our team such a powerhouse in reducing the ransom demand. This service also includes the facilitation of cryptocurrency, and running the payment through our compliance program.

Important: Fees for these services are open for negotiation for discounts with volume.

FAQ

How exactly do we benefit from this partnership?

SalvageData services offer a faster disaster recovery process with a higher success rate. With increased chances of recovery or decryption without ransom payment, plus our expert mediation services, our team will significantly lower your claims payable.

Why would I call you when I have someone local?

Having someone locally only goes so far, since it doesn't guarantee the same qualifications and efficiency that an expert service provider can offer. That said, should you need someone at the location, SalvageData can deploy an agent onsite within 24 hours of the issue being reported.

Every other company claims they can recover our clients' data, and they often can't. What's different about SalvageData?

SalvageData's mission is to get the most complex data loss scenarios and work tirelessly until 100% of the data is salvaged. Our experience allows us to diagnose the issue faster, decrypt most encryptions in-lab, and (if strictly necessary) negotiate a lower price on a

How fast can SalvageData decrypt ransomware-encrypted data?

The timeline of the recovery process can vary from 24 hours to 2 weeks. The complexity of the encryption plays a heavy part in determining if our technicians can reverse engineer the code, or decrypt with publicly available decryptors. Negotiations can also take anywhere from 72 hours to 2 weeks.

How likely are you to decrypt the data without paying the ransom?

In over 50% of the cases we've worked on, we've been able to decrypt critical data without engaging with the threat actor. This means that we were able to locate decryptors through our work with FinCEN and OFAC, among others. Or, in some cases, reverse-engineer a solution in our laboratory.

FAQ cont.

Isn't AES encryption so reliable and impossible to break?
In general, breaking AES encryption used in ransomware is very difficult due to the large key space that it uses. However, no encryption system is entirely foolproof. Although the probability of breaking AES encryption using brute force is incredibly low, our engineers and cryptologists are continually learning new techniques and trends, which makes the difference when decrypting AES.

What's so special about your negotiation tactics?
Our team is highly experienced in decrypting known ransomware variants and is well-regarded in the industry for our expertise. Threat actors understand that our expertise is not to be trifled with and we are able to thoroughly analyze the encryption, find weak spots, and confirm what kind of data is infected. In simple terms, we can spot when they are bluffing and we use that as an advantage. You can trust our team to negotiate a favorable outcome and reduce the ransom demand.

Isn't paying the ransom illegal?
Since 2020, FinCEN has determined it a crime to pay or negotiate with threat actors. SalvageData can legally assist ransomware victims in reducing the cost and making payments due to a compliance program our legal team has developed directly with FinCEN and OFAC.

How safe are SalvageData's Compliance and Risk Management practices?
Regarding SalvageData's Compliance and Risk Management practices, SalvageData is certified with several industry-standard security and privacy compliance certifications such as SOC 2 Type II, PCI DSS, and HIPAA, among several robust compliance and risk management practices implemented.

What are some other companies that you have worked with in the past?
Due to privacy clauses, we are unable to publicly name our past clients. We have served clients from various industries, including government, healthcare, education, and business. Please refer to our Case Studies section in this handbook to learn more about what kind of clients we've serviced and how we were able to help them.

What are your payment terms?
We offer a range of payment options, including PO for NET30, cards, wire, etc.

OUR LEADERSHIP TEAM

Bogdan Glushko

CIO & Head of Compliance

George Pavel

Director of Business Development

George Gershen

Director of Operations

THANK YOU

We believe in Trust and Integrity, Expertise and Leadership, Innovation and Collaboration, Excellence, and Quality. Eight great reasons to believe in us. Thank you for considering SalvageData as a partner. We look forward to providing you and your customers with quality ransomware removal solutions.

Bogdan Glushko

CIO & Head of Compliance

SALVAGEDATA

SALVAGE THE UNRECOVERABLE

SalvageData.com

@SALVAGEDATA

/SALVAGEDATA