LIFARS
your digital world, **secured**

RANSOMWARE ADVISORY

RANSOMWARE ADVISORY

LIFARS provides complimentary consulting on Ransomware attacks to determine if a move forward decision is desired with factors consisting of whether data exfiltration occurred, determining if additional systems have been compromised and/or requests to attempt data recovery.

For high profile ransomware cases LIFARS engages the U.S. Secret Service Electronics Crime Task Force which was formed to prevent, detect, mitigate and aggressively investigate attacks on the nations' financial and critical infrastructure.

KEY BENEFITS

1. **Assess recovery options/recommendation based on sensitivity/importance of data that is locked and identification of specific ransomware.**
2. **Recover private keys from recorded network conversations (provided client has a network recorder) and decrypt files without paying ransomware.**
3. **Determine whether to kill the process on all systems if it is still running or let encryption finish if paying ransom is the only remaining option.**
4. **Provide Advisory and/or additional assessment to determine IVoC and potential lateral spread.**
5. **Preserve system before recovery and consider full disk images for future analysis.**
6. **Conduct digital forensic investigation related to initial vector of compromise, initial system of entry, and possibility for sensitive data exfiltration.**
7. **If needed, forensic report is created for court of law, legal and insurance claim purpose.**
8. **Scan all relevant systems with collected IoC for potential existence of scheduled malware triggers, provide findings and/or conduct remediation.**
9. **Determine what could have been done to avoid the ransomware attack based on identification of IVoC, if it can be determined.**
10. **Consult with client with regards to reporting to police or federal authorities.**

LIFARS
your digital world, **secured**

RANSOMWARE ADVISORY

LIFARS EXPERTISE

Ondrej Krehel, CEO & Founder developed LIFARS proprietary forensics methodology over a span of 20 years leading and working on High-Profile cyber security engagements and initiatives around the world. He is a Subject Matter Expert in the fields of Digital Forensics and Cyber Resiliency and holds a multitude of significant Information Security certifications including the esteemed Certified Hacking Instructor, CEI status. The LIFARS forensics' experts have experience and acknowledgment across the spectrum of the military intelligence community, and international alliances such as NATO, Interpol and Europol. We have remediated several complex high-profile investigation cases that have hit the news media headlines. Our work covers the scope of proactive and reactive engagements which often require attention of the FBI, CIA, NSA and more.

ABOUT LIFARS

LIFARS is a global leader in Incident Response, Digital Forensics, Ransomware Mitigation and Cyber Resiliency Services. LIFARS investigates hundreds of incidents each year. Our reputation is known world-wide, and LIFARS expertise is called on by intelligence agencies such as the FBI, Homeland Security, Secret Service, and Interpol. LIFARS executes with military speed, precision, and expertise. Results matter, and your reputation is as valued as ours.

The LIFARS New York Laboratory is an industry pioneer in developing methodologies to identify indicators of compromise and threat actors, including those backed by nation states. LIFARS has investigated and responded to all types of cyber threats from intellectual property theft, extortion, hacking of celebrity social media accounts, money transfer, to serious breach attacks and sabotage from nation states.

Speed

Time is money. LIFARS gets you back up running swiftly and securely.

Precision

LIFARS collects evidence for prosecution where others have failed.

Expertise

LIFARS has elite knowledge and insight called upon by intelligence and law enforcement agencies.

CERTIFICATIONS

ACE | CCFP | CCNA | CEH | CEI | CISA | CISM | CISSP | EnCE | GWAPT | KLCP | PMP | SCJP

CompTIA Security+ | CIPP | CRISC | PCIP | C/CISO | ITIL | CGEIT

Contact LIFARS to Learn More
www.lifars.com | 212.222.7061 | info@lifars.com