CRYPSIS™

DATA SHEET

Ransomware Investigation and Recovery

The Crypsis Group's Ransomware Investigation and Recovery service helps organizations investigate, eradicate, and recover from ransomware attacks. Crypsis has experience helping organizations respond and recover from ransomware infections ranging from one to hundreds of systems.

HOW WE CAN HELP

INVESTIGATE

- Conduct forensic analysis of systems infected with ransomware to identify:
  - Initial infection vector
  - Potential data exposure
- Perform micro-investigations to determine:
  - Initial access into the environment
  - Impacted systems and user accounts
- Reverse engineer malware to determine the following:
  - Indicators of Compromise ("IOCs")
  - Ransomware capabilities

ERADICATE

- Develop and implement a containment plan to isolate additional infections
- Assist in the removal and cleanup of ransomware
- Provide strategic recommendations to mitigate the impact of future infections
- Review the organization's susceptibility to ransomware attacks

RECOVER

- Facilitate cryptocurrency payments for encryption keys to recover data
- Assist with data recovery based on the organization's disaster recovery technology

RECOVERY PROCESS

The Crypsis Group acts on behalf of our clients to undertake the following:

1. Initiate communication with the bad actor to obtain decryption utility

2. Obtain proof of file decryption

3. Facilitate cryptocurrency payments on behalf of victim to obtain a decryption utility

4. Perform code analysis on the decryption utility to ensure no malicious code exists

5. Provide tutorial to the victim to demonstrate how to decrypt their files

6. Provide remote troubleshooting support

WHY CRYPSIS

Breadth of Knowledge

Members of the Crypsis team have responded to and managed investigations of complex data breaches at global organizations across multiple industries. We have responded to data breaches of all shapes and sizes and are experienced at responding to compromises involving cloud-based applications and enterprise applications. We have experience responding to attacks by nation-state actors, insiders, and thieves looking to steal PII, PCI, and PHI data.

Operational Expertise

We are operational security experts. We have stood up SOCs and run those operations. We know how to spot malicious threat actors and what to do to prepare for the worst. We understand that effective security programs improve the organization's security posture without compromising the functional needs of the business. We work with our clients to provide actionable and realistic recommendations to achieve those objectives.

Perspective

We understand what our clients go through. A number of our consultants have been on the other side of data breaches, having lived through some of the largest commercial data breaches on record. We bring this perspective to each of our engagements, offering clients insights into how to deal with the components one must deal with when preparing for and managing an incident.

Security for Every Budget

We believe organizations of all sizes should have access to the expertise they need to be as secure as they can be. We work with our clients to establish a budget that makes sense for them.

Contact Us to Learn More About The Crypsis Group

703.570.4103 | info@crypsisgroup.com

The Crypsis Group is a security advisory firm focused on supporting our clients as a trusted advisor before, during, and after a breach. The combination of our deep security knowledge, proprietary technology, and methodology allows us to rapidly identify, contain, and eradicate attacks for organizations. Our team's experience spans security monitoring within the intelligence community and advising at the national security level to performing high profile data breach investigations and leading remediation efforts.