DigitalForensics

VESTIGE Digital Investigations

# Incident Response Service Offerings

## Computer Triage

Deployment of Vestige virtual device containing tools to analyze client environment. Triage of devices in environment to gain insights on:

- Initial attack vector
- Candidate devices for thorough analysis
- Evidence of unauthorized individuals in environment
- Scope of infected devices

The goal of the triage is to get an assessment of the scope of potential damage as well as identification of devices to examine in greater detail.

## Forensic Analysis

Capture of memory and disk images for thorough analysis. Review of devices to determine scope of involvement such as:

- "Patient 0", the first computer infiltrated from which the unauthorized individuals started their attack.
- Devices containing unauthorized malware such as:
  - Remote access for unauthorized individuals
  - Crypto-currency mining
  - Keylogger
  - Bot Software
- Devices showing evidence of data exfiltration
- Devices involved in execution of ransomware

## Log File Analysis

Analysis of log files to determine evidence of unauthorized access or data exfiltration. Potential sources of analysis include:

- Office 365 Audit and Mailbox Audit logs
- Firewall and VPN logging
- Web server
- Cloud service providers including Dropbox, AWS and others

Analysis is dependent on available information due to settings, retention policy, etc.

## Malware Analysis

Analysis of malware binaries and scripts to determine their purpose and identify any logical errors which could alter their intended purpose.

**Contact Vestige today to discuss your Incident Response needs.**

*TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™*

info@VestigeLtd.com | **800.314.4357** | www.VestigeLtd.com