



INCIDENT RESPONSE & FORENSICS ANALYSIS

Donald J. Fergus

Intekras, Inc.
21515 Ridgetop Circle
Suite 260
Sterling, VA 20166
(703) 547-3500
www.intekras.com

March 2010

white paper





Insight. Innovation. Integrity.

- Information Assurance
- Technical Services
- Workforce Development

WHITE PAPER

Table of Contents

External Discovery..... 1

Network Discovery (Foot Printing)..... 2

Malware Analysis..... 3

Forensic Analysis..... 4

On-Site/On-Call Cyber Incident Response Analyst..... 5

About Intekras..... 7

The Intekras Incident Response and Digital Forensics services can be performed on both a “pre-event” and “post-event” basis. In either case, our experts are able to lead you to an improved security posture and a more hardened architecture, trend knowledge regarding traffic and activities affecting all departments, enclaves, or trading partners, and an overall improvement in your ability to prevent, detect, protect, and respond to data breaches, malware attacks, denials of services, and other cyber attacks.

The Intekras Pre-Event Capabilities include the following:

External Discovery

Intekras is able to perform “zero-knowledge discovery” activities involving network reconnaissance and gathering information using techniques such as Google Hacking, WHOIS Interrogation, DNS Interrogation, Traceroute, and other Internet queries.

The purpose of an External Discovery search is to identify sensitive information about an organization in a non-intrusive manner using publicly available sources. All companies must classify and maintain their data so that internal information, such as trade secrets and financial data, is not disclosed while external information, such as a company’s mission statement or product data, is widely accessible. When data is not properly classified and the security controls that surround these two data sets are not properly implemented, sensitive information about an organization may be revealed. Information that is unintentionally disclosed by a company is often referred to as “information leakage.”

A company’s information can be organized into several categories. These include information about people, technology and intellectual property. For each of these categories, both internal and external information must be maintained:

- **People**

External disclosure: names and contact information for company management, marketing, human resources, etc.

Internal retention: names and details of individual employees

- **Technology**

External disclosure: public web servers, mail gateways, etc.

Internal retention: intranet web servers, database servers, directory servers, etc.

- **Intellectual Property**

External disclosure: white papers, technology overviews

Internal retention: technical documents, source code, customer lists, etc.

Intekras performs External Discovery searches that attempt to identify items that would be considered as part of a company’s “information leakage.” Intekras focuses these searches on information that should never have been disclosed but can be found by scouring public sources that are accessible on the Internet.

Below is a list of information sources that Intekras uses during an External Discovery search:

Network Registries: The domain name and Internet address registries provide broad information about the network names and addresses that have been assigned to a company. The Internet

Assigned Numbers Authority (IANA) maintains links to the individual registries that assign Internet network address ranges and manage domain names. Information can be queried in real-time using the “WHOIS” system.

DNS Records: Each organization must maintain entries in the Domain Name System (DNS). A company’s primary Internet name (such as “google.com”) must have DNS records so that web sites, email gateways, and so forth can be reached. However, DNS records may reveal information about a company’s network infrastructure, architecture, or internal systems as well.

Web Content: Use is made of a standard Internet browser, e.g. Firefox, Chrome, Opera, or Explorer to examine web-pages relating to the organization.

Job Postings: Job listings posted by an organization may provide insight into the types of technologies and intellectual capital that a company has by revealing a list of desirable skills needed for applicants. Likewise, resumes posted by former employees may include extensive information about the internal systems of their prior employer. For example, a resume may discuss specific projects worked on and the technologies used.

Common sources of job posting data include job search web sites such as “monster.com.” Also, the web sites of newspapers in locations where companies have large offices may also contain this information. For example, the Washington Post maintains an online job database.

Online Discussions: Company employees often participate in online discussion forums using company supplied equipment or email addresses. By searching for company email domains or employee names throughout these forums, internal company information may be obtained. Online discussion forums include newsgroups (NNTP internet standard), mailing lists (email broadcast lists, with public/searchable archives), discussion boards, and Social Media postings.

Internet Archive: The Internet Archive contains “snapshot” copies of web sites as they appeared at specific points in time. By using the archive, it is often possible to view old web pages previously published by a company. These old pages may contain information that has removed or reverted to internal-use only. Google’s sophisticated web caching technologies can also provide a view into old versions of a company web presence.

Bogus Domains: While a company may maintain many Internet domain names, other individuals having no relation to the company may also attempt to register domain names for the company and provide false or misleading content on web sites. These fake or unauthorized domain names may be slanderous in nature, may be variations in the spelling of a company’s name, may use different top level domains (such as .info or .biz) or may be registered in foreign countries (such as .uk or .cn).

While the purpose of an OSINT search is to obtain information in a “Blackbox” manner without any access to organization resources, having some data up front can assist Intekras in identifying the most critical information leakage. For example, a client could provide a list of code words, a small excerpt of proprietary source code, or a sampling of employee names.

Network Discovery (Foot Printing)

In this effort, Intekras performs external network discovery (also known as “foot-printing” or “network mapping”) to gather data on all active device addresses and network services accessible from the

public Internet. A Network Discovery is the process of identifying and evaluating all network assets, and we start by establishing a map or “fingerprint” of the targeted network segments.

Information about the target IP segments may be provided by the client in the form of an Internet Protocol (IP) network address range, list of individual IP addresses, network architecture diagram, or similar format. If the customer desires this portion of the assessment to be performed as a “Blackbox” assessment, Intekras will supply the client with a list of identified subnets and Internet facing hosts we believe belong to them. This list will be the result of our OSINT findings and other research techniques we will use to passively identify client’s Internet facing systems without the use of scanning tools.

After review and approval by the client of the submitted list Intekras will then proceed on to the scanning phase of this task. The purpose of the approval process is to ensure that all potential target information is confirmed with the customer prior to the initiation of any tests or scans to ensure a limited risk of misdirected network traffic.

All active device addresses and their associated Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and other network services accessible from the target network within the specified range will be discovered during this effort. Where an accessible network service is detected, positive identification is established through analysis of any protocol negotiation and connection using appropriate client software.

Probes using the Internet Control Message Protocol (ICMP) to determine device availability, response latency, timestamp information, and potential network routing / filtering devices will also be recorded.

Our Network Discovery toolset includes several COTS, Open Source, and proprietary scripts and assessment tools, including Nmap, Qualys, Nessus, Ethereal, Firewalk, Hping/Fping, etc.

The Intekras Post-Event Capabilities include the following:

Malware Analysis

The threat of malicious software can easily be considered as the greatest threat to Internet security. In the past, viruses were the only form of malware. Today, the threat has grown to include network-aware worms, trojans, DDoS agents, IRC Controlled bots, spyware, and so on. The infection vectors have also changed and grown and malicious agents now use techniques like email harvesting, browser exploits, operating system vulnerabilities, and P2P networks to spread.

Intekras is able to provide expert Malware Analysis support through the use of its state-of-the-art Digital Forensics Lab in Sterling, VA. Through the use of controlled and sanitized Lab, Intekras is able to:

- Create a controlled environment for Malware Analysis
- Baseline images, files, registries, and other configuration data
- Collect information in a “forensically sound” manner
- Analyze information using the most current tools
- Fully document the results/evidence

Initially, Intekras is able to eradicate Malware from all infected hosts. During this phase we may be required to delete files, registry keys or even possibly rebuild the infected host or hosts. During this “eradication phase”, we shall work with system administrators to make a determination of when the

malware infected the compromised host or hosts, as well as if the host backups are infected.

With the malware eradicated, Intekras then moves into a “recovery phase” of the analysis effort. At this point, if an anti-virus vendor has released a signature for the malware, we shall ensure that the updated signature should be installed on all hosts. Additional actions may include deploying an IDS rule that detects send/receive activities aligned with the malware (e.g., abnormal outbound SMTP traffic). Firewall logs will also be closely monitored during the recovery phase for any unauthorized traffic.

At this point, the malware is then brought into the Intekras Lab. Our goal is to gain an understanding of how a specific piece of malware functions so that defenses can be built to protect an organization’s network. There are two key questions that must be answered. The first: how did this machine become infected with this piece of malware? The second: what exactly does this malware do?

There are two types of malware analysis that Intekras performs in its Lab: code (or static) analysis and behavioral (or dynamic) analysis. Code analysis is the actual viewing of code (through reverse engineering and/or disassembling) and walking through it to get a better understanding of the malware and what it is doing, while behavioral analysis is how the malware behaves when executed (through the “sandboxing” of the malware on a baselined system), who it talks to, what gets installed, and how it runs. When performing malware analysis, Intekras performs both static and dynamic analysis to gain a complete understanding on how a particular malware functions.

The tools we use in Malware Analysis are quite extensive, and include the following:

- Behavioral Analysis: BgInfo, Process Explorer, Process Monitor, RootkitRevealer, Streams, Strings, TCPView, Windump, Fport, Hfind, Vision, Filewatch, MD5sums, Winalysis, WinHex, etc.
- Code Analysis: IDA, Reverse Engineering Compiler, ProcDump 32, PE Explorer, Livekd, Debugview, etc.

Forensic Analysis

In this effort, Intekras analyzes system and security event data for trends, intrusions, anomalous behavior, strange log patterns, and other events and activities that signify the need for some level of IT security triage or incident response in accordance with industry best practices. We then categorize them using industry best practices and US-CERT guidance, sort them by client location or organizational structure and provide high-level recommendations for how to handle the events/incidents. These recommendations may include improved incident handling procedures, log setting changes, or security architecture recommendations, and so on.

The Intekras forensic experts take a very in-depth and structured approach to forensic investigations. Intekras forensic analysts gather all the relevant technical information available in order to identify all sources of documentary or digital evidence. This process aids Intekras forensic analysts in building a greater understanding of the security incident being investigated. The sources of information include, but are not limited to, the following:

- Security device logs (Firewall, Intrusion Detection/Prevention System, DLP device)
- Remote Access device logs (Virtual Private Network, RAS, local system)
- Operating System security and event logs (Windows, UNIX, other platforms)
- Physical security device logs (badge readers, biometrics controller output)

The unique range of technical knowledge Intekras consultants have in all areas of Digital Forensics, Information Security and general Information Technology gives the Intekras team a much better understanding of the underlying fundamentals of each engagement, as well as the ability to “come up to speed” much quicker.

Once gathered, evidence is examined for significant content, correlated and matched to investigation findings. Analysis activities are dependent on the precise investigation scope, but may include the correlation of multiple events to singular actions (i.e. unauthorized system access, data manipulation) and development of potential incident reconstruction scenarios to analysis of raw hard drive images to detect hidden data. All questionable or suspect information will be thoroughly documented, evaluated, analyzed and assigned significance throughout the course of the analysis. In addition, strict adherence to chain of custody rules shall be adhered to.

The analyzed data will be used to construct a timeline showing possible event reconstructions to display possible scenarios. The timeline defines specific security incidents, methods of unauthorized activities, potential suspect systems or users and possible intruder activities outside of the network.

All applicable technical data discovered will be documented and presented in a manner that is clear, concise and understandable by the non-technical person. The report will be presented as a logical and chronological story of the events comprising the incident, as well as technical information concerning the details of the incident. The report will be delivered within two weeks of the end of the investigation, and a briefing containing any pertinent data will be given to the client upon the conclusion of the analysis. Remediation strategies are proposed to prevent additional unauthorized activities through the same method.

Intekras uses a variety of legally recognized commercial and open source tools in its investigations, including the following:

- **Sniffers, Loggers, Analyzers:** NetworkMiner, NetIntercept, WireShark, Ethereal, Air PCAP, Kismet, Xplico, netcat, tcpdump, etc.
- **Log Analysis:** Centrifuge, Splunk, AnaLog, Log Parser, etc.
- **Media/Network Analysis:** EnCase, FTK, CellDek Tek, LogiCube Talon, NetWitness, Live Response, etc.

Please note that all investigations are assumed to be evidentiary investigations unless informed otherwise by the client, and Intekras handles them as such. An evidentiary investigation assumes that the client wishes to prosecute the offending individual, and there are formal legal steps required in order to maintain the chain of custody of evidence and preserve the integrity of the data. Intekras is fully capable of investigating an incident and providing professional testimony in court proceedings. The Intekras Digital Forensics Lab, located at Intekras headquarters in Sterling, VA is accredited to process and store classified information at the SECRET level and contains a GSA-approved Class 5 safe for the secure physical storage of hardcopy and electronic media.

Finally, Intekras is able to dedicate a Digital Forensics expert to our clients:

On-Site/On-Call Cyber-Incident Response Analyst

In this effort, Intekras assigns an IT Security Specialist, who is capable of assuming all the pre-

event and post-event tasks listed above. The Analyst shall respond to suspected incidents and coordinate appropriate actions with required agency or other client personnel as needed. The Intekras Analyst can serve as an IT Security Office point of contact for notification and reporting of all computer/network security related events and incidents.

Our Analysts can be made available on a 24/7 basis, and facilities can be set up so as to allow the Analyst to immediately receive and disseminate incident information and provide a consistent and timely capability to respond to and report on incidents.

Furthermore, the Intekras Analyst can perform the following activities:

- Respond and report in compliance with SANS Institute, DoJ, and Federal Rules of Civil Procedure guidance and regulations;
- Prepare incident reports in accordance with US-CERT guidance and appropriate for submission to US-CERT
- Communicate with IT Specialists, Outsource Vendors, and SOC personnel regarding incident prevention, detection, protection and response activities
- Communicate event and incident findings to all levels within a client organization – from executives to system administrators
- Advocate the use of industry and legal standard evidence preservation techniques for properly maintaining chain of custody
- Develop a baseline detailed inventory of the client IT products, versions, operating systems, locations, etc.
- Implement processes to ensure the organization subscribes to product and security vendor vulnerability notification data (e.g., CVE, CWE, NVD, OPAL, etc.) relevant to the detailed inventory of the client's IT products
- Coordinate the collection and analysis of logs, web filters, packet traces, raw dumps, etc. to produce monthly usage, trend, event, and other analytic reports.

The Intekras Incident Response/Digital Forensics service provides support to customers who require preventative analysis or an in-depth investigation of a computer security incident. Such incidents can include possible misuse of company resources by employees, malicious activity by employees, possible compromise of sensitive information or malicious network traffic. Handling an information security incident requires careful treatment of evidence and a thorough investigative process. Should a client need assistance in investigating internal resource misuse, possible policy abuse or responding to a computer security or possible hacking incident, Intekras can help uncover the reasons behind a security breach as well as offer assistance in remediation. Further, through the Intekras Digital Forensics Lab and Field Toolkits, we offer customers and unparalleled level of engineer interaction while on-site and during the evidentiary analysis phases of investigation.

Conveniently located in the Loudoun Technology Center in Sterling, Virginia, Intekras is a privately owned small business, offering integrated solutions in Information Assurance & IT Risk Management, Technical Services and Workforce Development.

Our executive team has over 125 years of combined experience in our core disciplines. Intekras has an outstanding track record in the public sector including DHS, DoD, Navy, Army, HUD, Peace Corps, HHS, OPM and VDOT as well as strong past performance with such companies as Northrop Grumman, Lockheed Martin, SRA International, Raytheon and others. Our private sector experience includes such Global 100 & Fortune 500 companies as Citibank, AOL/Time Warner, Bridgestone and others.

Intekras: bringing insight, innovation and integrity to your business and technology challenges.

