

Anatomy of a Data Breach...and How to Prepare for One

STROZ FRIEDBERG

Kenneth A. Mendelson, CISSP, CIPP
Managing Director



Randy V. Sabett, J.D., CISSP
Vice Chair, Privacy & Data Protection

DATE: June 9, 2015



LEVEL SET: BOARD AND MANAGEMENT CONSIDERATIONS



1. Create Governance Structure
2. Research Threats
3. Prioritize Information Assets
4. Perform a Risk Analysis
5. Create a Security Plan Tied to a Technology Acquisition Strategy
6. Engage Third Parties Appropriately (legal, technical, procedural)
7. Request Regular Updates and Adjust Accordingly
8. Test the Response Plan
9. Maintain Appropriate Insurance Coverage
10. Regular Training for Employees, Vendors, and Other Third Parties



QUESTIONS BOARDS SHOULD CONSIDER ASKING

1. Has Management identified known risks to the Company?

- A. cybercrime, accidental failure, insider threat, nation-state attack, issue-based attack, or other
- B. What are the crown jewels?
- C. Biggest vulnerabilities? (IT Systems, people, third parties)
- D. CS Legal obligations (from regulators or customer contracts)
- E. CS events within company or in its sector?
- F. What CS testing has been done?
- G. Progress along maturity model.
- H. Others?

2. Are appropriate safeguards in place?

- A. (Program, resources, training, vendors, etc.).
- B. Insurance in place?

3. Can management detect cybersecurity incidents?

4. Has management implemented an IR plan?

5. Is there a plan to recover and restore after an incident?

Data Breach – Checklist of Initial Steps


In Advance:

- ☐ Form Team – Legal, IT, HR, Compliance/Security, Public Affairs, Outside Expert.
- ☐ Send email from management to team, addressing needs and lines of authority.
- ☐ Prepare memo of relevant law(s) and contractual obligations.
- ☐ Prepare "Red Flags" memo, describing events that need to be escalated.
- ☐ Distribute expected timeline of events to the team.
- ☐ Create contact lists of: a) team members, b) affected partners, 3rd parties.
- ☐ Create list of needed facilities and equipment.
- ☐ Identify your most critical data locations (e.g. credit card server).
- ☐ Distribute backup schedule for key data; test time it takes to restore data.
- ☐ Review current user list to see if it's current (purge old accounts).
- ☐ Centralize administration of computer logs.
- ☐ Synchronize network clock times.
- ☐ Assemble team to review duties and first steps in the event of a breach.

When a Breach Occurs:

- ☐ Assemble team, distribute list of responsibilities.
- ☐ Unhook infected machines (pull network cord from wall, leave power on).





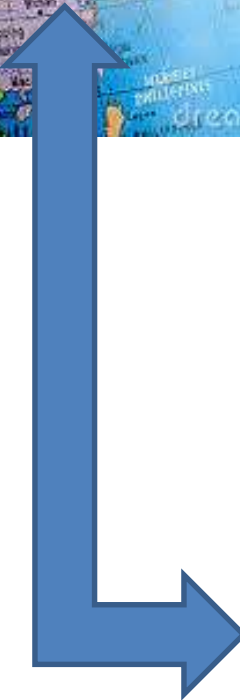
ANATOMY OF AN INCIDENT



High-tech and investigative experts respond to, remediate, and help resolve an array of cyber-related incidents including:

- Data Breach
- Advanced Persistent Threat
- Lost Laptops, Servers, Backup Tapes
- Leaks of Confidential Information
- Theft of IP & Trade Secrets
- Identity Theft
- Industrial Espionage
- Hacks, Unauthorized Access, Exceeding Authorized Access
- Spyware & Other Invasive Software
- Botnets and Malicious Code
- Denial-of-Service (“DDoS”)
- Cyber-extortion & Cyber-harassment
- Click Fraud & Affiliate Marketing Fraud

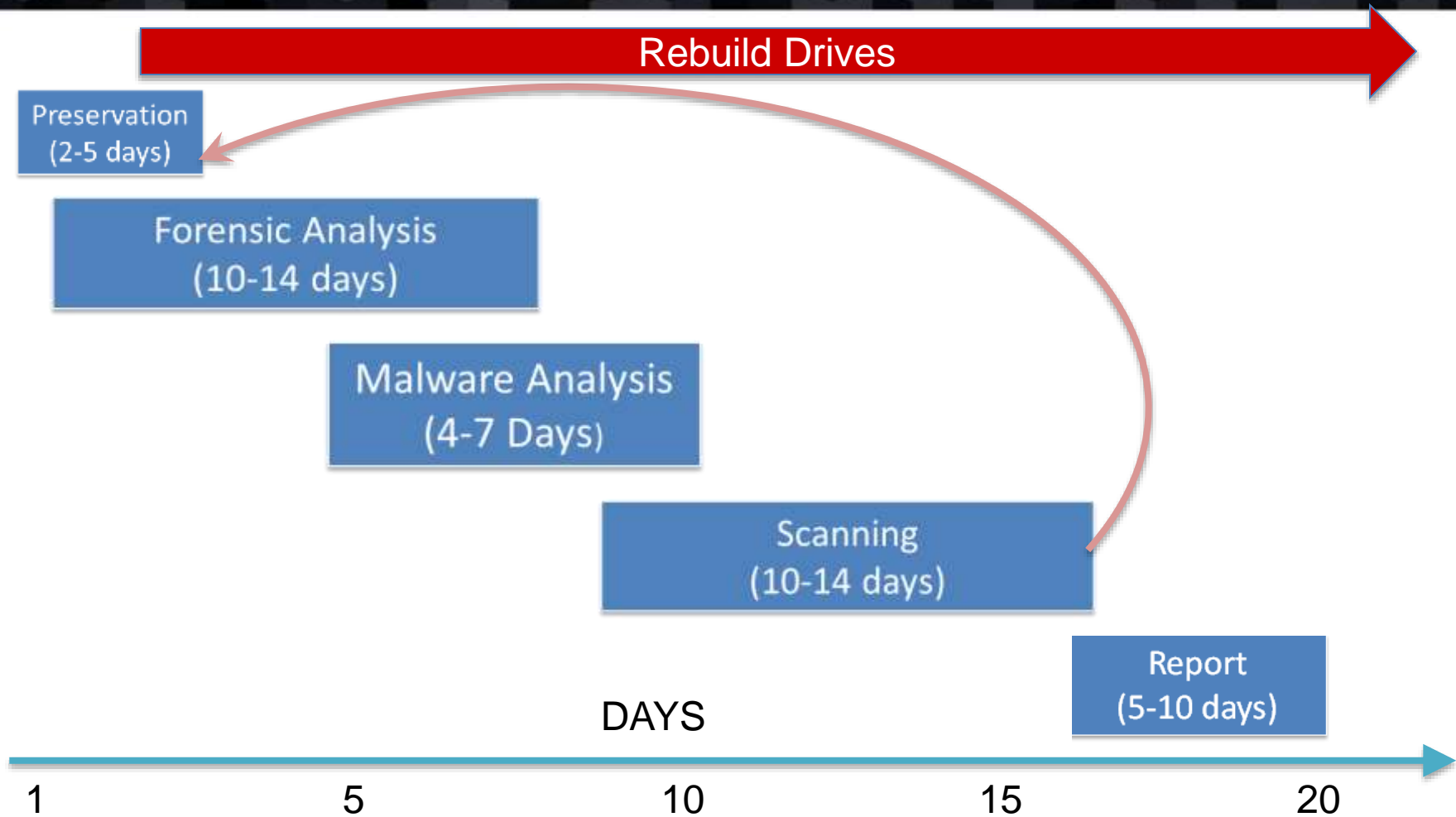
SCENARIO



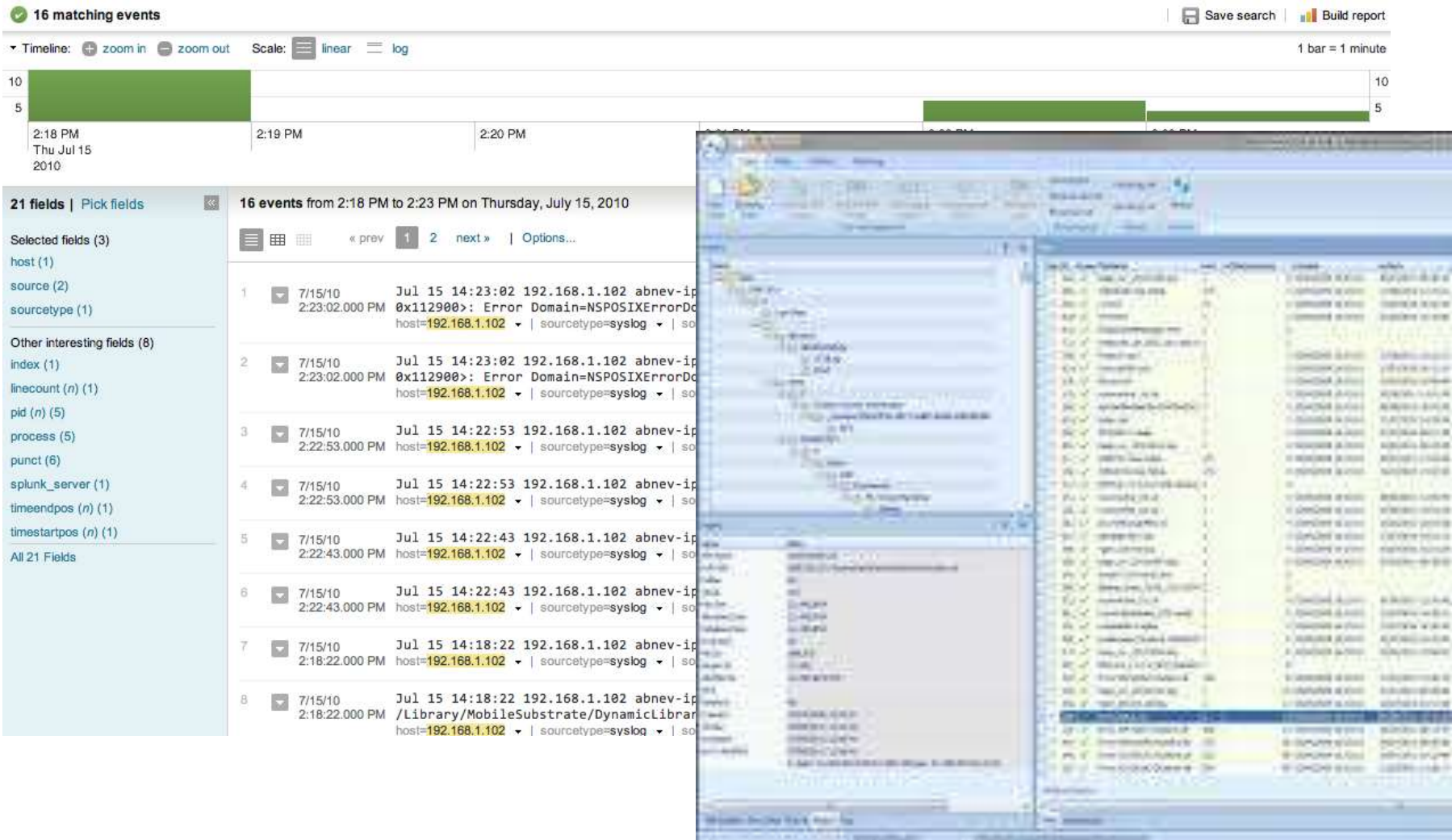
- Test interview reports via sampling.
- Analyze log files/Set up sniffers
- Review memory/virtual memory.
- Analyze hard drives.
- Analyze and reverse malware code.
- Review live traffic captures.
- Scan hosts for IOCs
- Remediate
- Repeat as needed



BREACH RESPONSE TIMELINE



Analyze available network logs



Set up network sniffers to evaluate ongoing activity, capture packets, etc:



OmniPeek

File Edit View Capture Send Monitor Tools Window Help

WildPackets OmniPeek

Start Page **Capture 1**

Packets received: 1,204,015 Buffer usage: 100%
Packets filtered: 1,204,015 Filter state: Accept all packets

Stop Capture

Dashboards

- Network
- Voice & Video
- Apdex

Capture

- Packets
- Log
- Filters

Expert

- Hierarchy
- Flat
- Application

Web

- Servers
- Clients
- Pages
- Requests

Voice & Video

- Calls
- Media

Visuals

- Peer Map
- Graphs

Statistics

- Nodes
- Protocols
- Summary

Flows analyzed: 3,765 Events detected: 9,432
Flows recycled: 0 Packets dropped: 0

Client Addr	Server Addr	Flows	Events	Packets	Bytes	D
0.0.0.0	0.0.0.0	3	0	9	1964	0:02:22.6
0.0.0.0	IP Broadcast	1	0	22	7612	0:05:14.9
10.3.2.21	10.4.58.3				66	0.0
10.3.2.67	10.4.58.6				114	0.0
10.3.5.87	10.4.3.45				14872	0:08:10.5
10.4.1.8	10.4.58.81				197	0.0
10.4.2.100	10.4.255.255				494	0.0
10.4.2.116	10.4.58.3				6332	0:06:45.1
10.4.2.116	10.4.58.6				22822	0:08:00.0
10.4.2.116	10.4.255.255				2798	0:03:33.0
10.4.2.116	66.225.202.210				134588	0:02:36.2
10.4.2.116	66.225.202.213				10701	0:01:35.9
10.4.2.116	69.90.236.49				54606	0:08:30.2

Visual Expert

- Expand All
- Collapse All
- Save Flow Statistics...
- Select Related Packets
- Show Address Names
- Show Port Names
- Make Filter...
- Insert Into Name Table...
- Resolve Names
- Expert View Options...
- Network Policy...
- EventFinder Settings...

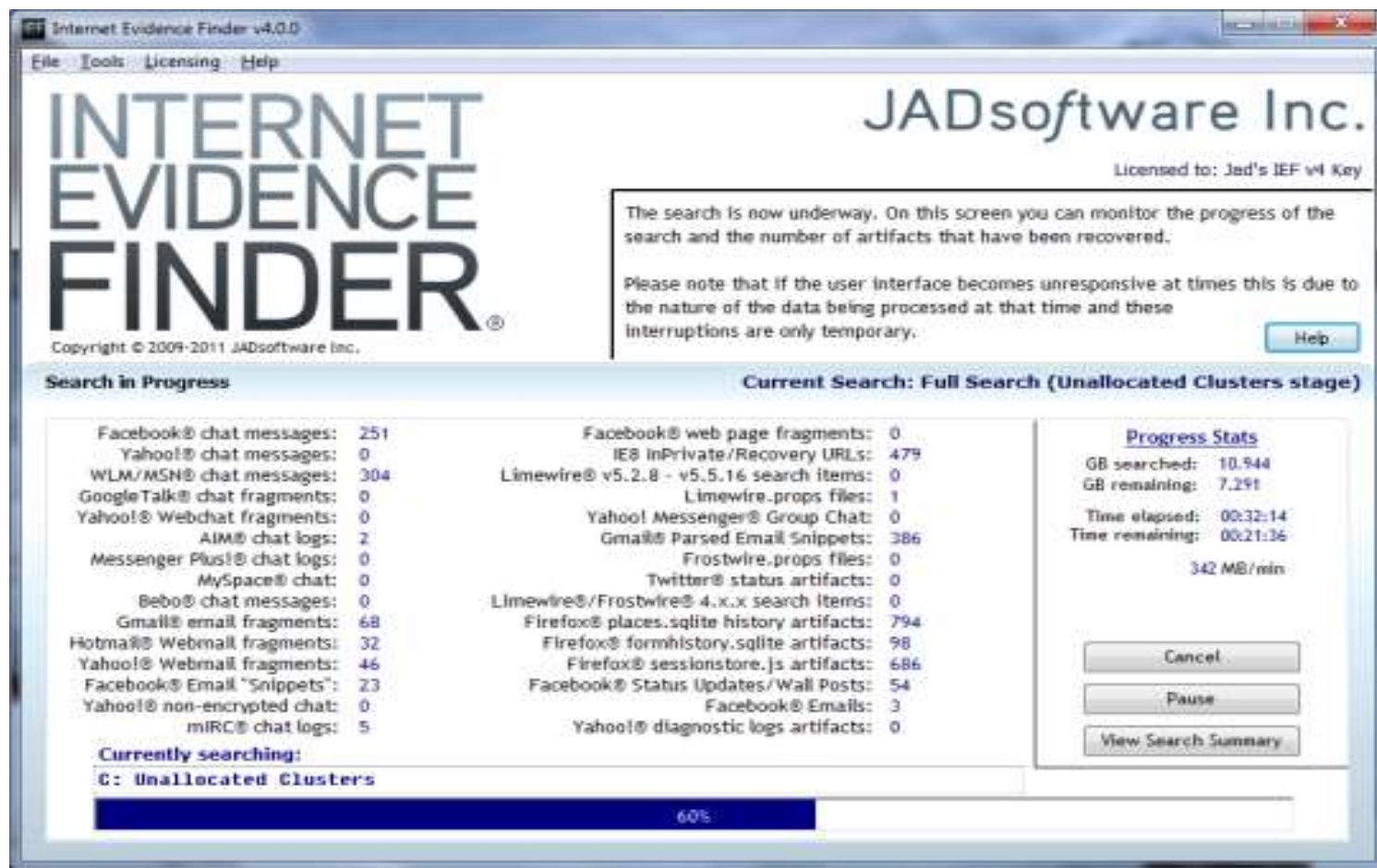
Details Event Summary Event Log

	Client	Server
Name	10.3.2.21	10.4.58.3
Network Address	10.3.2.21	10.4.58.3
Packets Sent	1	0
Bytes Sent	66	0
Average Size (Bytes)	66	-
First Packet Time	1/12/2009 14:44:54	-
Last Packet Time	1/12/2009 14:44:54	-
Routed Hops	0	-
TCP Min Window	-	-
TCP Max Window	-	-

Capturing Local Area Connection Packets: 88,723 Duration: 0:09:06

For Help, press F1 Wireless Network Connection Channel: 124 - 5620 MHz (a)

INVESTIGATE SUSPICIOUS INTERNET ACTIVITY



FORENSIC ANALYSIS

















Volatile Data Capture

Capturing physical memory may reveal processes not normally seen by user or IT.

Proc#	PPID	PID	Name:
0	0	0	Idle
1	0	8	System
2	8	156	smss.exe
3	144	164	winlogon.exe
4	144	168	csrss.exe
5	156	176	winlogon.exe
6	156	176	winlogon.exe
7	156	180	csrss.exe
8	176	228	services.exe
9	176	240	lsass.exe
10	1112	284	dd.exe
11	820	324	helix.exe
12	228	408	svchost.exe
13	228	436	spoolsv.exe
14	228	464	Avsynmgr.exe
15	228	480	svchost.exe
16	228	540	regsvc.exe
17	228	552	MSTask.exe
18	228	592	dfwrs2005.exe
19	464	612	VsStat.exe
20	464	628	Avconsol.exe
21	600	668	UMGR32.EXE
22	228	672	WinMgmt.exe
23	800	820	Explorer.exe
24	820	964	Apoint.exe
25	820	972	HKserv.exe
26	820	972	HKserv.exe
27	820	988	DragDrop.exe
28	820	1008	alogserv.exe
29	820	1012	tgcmd.exe
30	820	1048	PcfMgr.exe
31	408	1064	JogServ2.exe
32	864	1072	Apntex.exe
33	820	1076	cmd.exe
34	592	1096	nc.exe
35	324	1112	cmd2k.exe

SEARCH for Deleted Data

Deleted Files: Hacker's Toolkit

Name+	Type	Size
 EraseLog.vbs+	VBScript Script File	1,109
 FindPass.exe+	Application	17,408
 Letmein.exe+	Application	18,432
 ListAdmins.vbs+	VBScript Script File	1,213
 Netsvc.exe+	Application	14,336
 NETVIEWX.EXE+	Application	40,960
 Psexec.exe+	Application	90,112
 PsKill.exe+	Application	26,624
 Psloggedon.exe+	Application	45,056
 pspasswd.exe+	Application	57,344
 Pulist.exe+	Application	55,296
 rasmon.dll+	Application Extension	4,608
 rasmon.exe+	Application	16,384
 Sqlrcmd.asp+	ASP File	4,004

Social security number:

=== - == - ==, == == ==, ==, ==,
“SSN, Social Security Number, socsec,” etc.

Credit card number:

5411222233334444 = 5.41122E+15 in scientific notation

Unsearchables:



SSN 000-00-1234
SSN 000-00-5678

MALWARE REVERSE ENGINEERING

Behavior Analysis

Process: sample4.exe, PID: 656

Process: _i.tspac7d.exe, PID: 1492

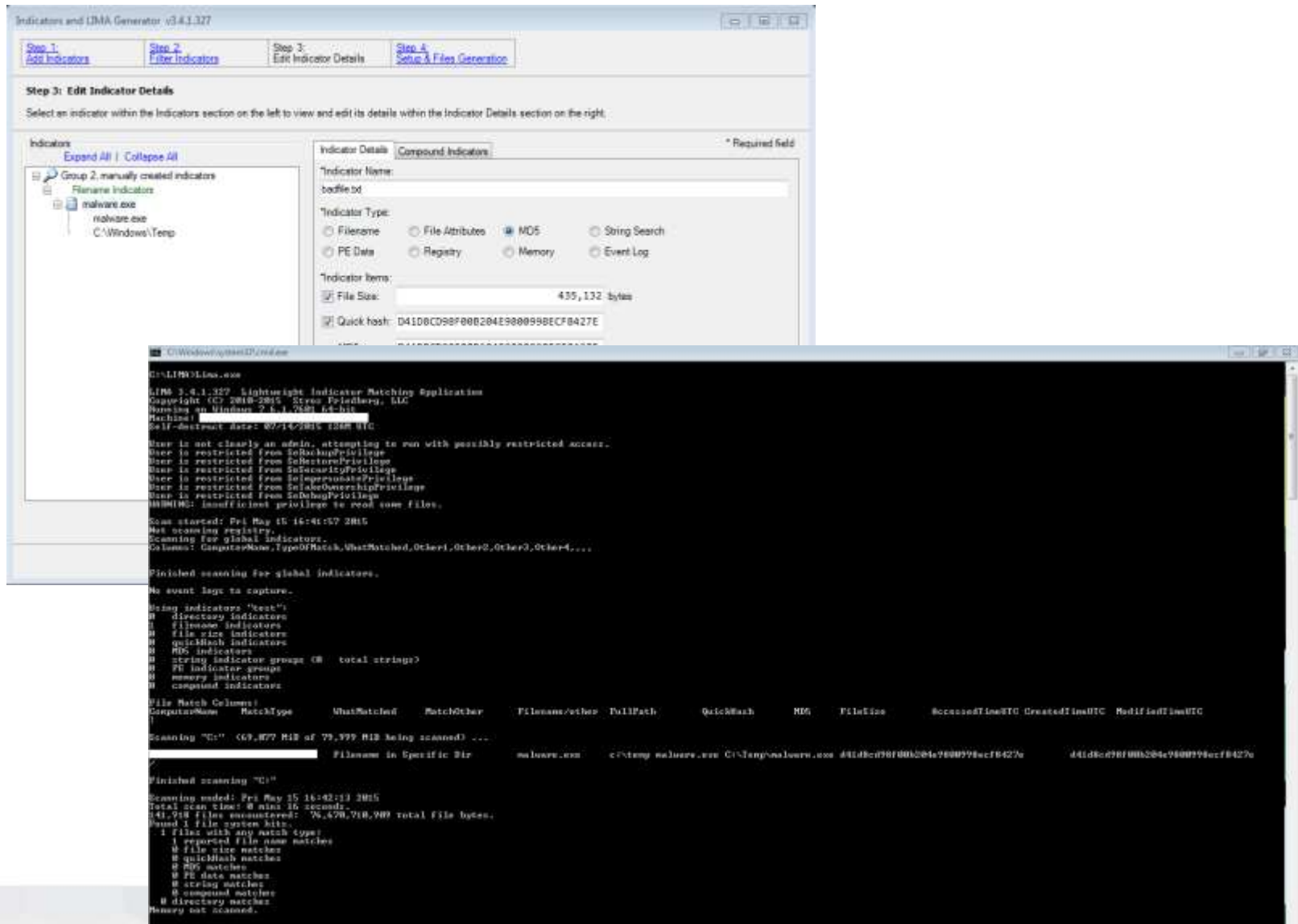
Timestamp	Function	Arguments	Status	Return	Repeated
03:43:17:807	DeviceIoControl	hDevice => 0x00000770 dwIoControlCode => 0x00228144 lpInBuffer => 0x011b2ee0 nInBufferSize => 0x00000028 lpOutBuffer => 0x011b2ee0 nOutBufferSize => 0x00001000 lpBytesReturned => 0x013a7f98 lpOverlapped => 0x77e46700	FAILURE		
03:43:17:807	DeviceIoControl	hDevice => 0x00000770 dwIoControlCode => 0x00228144 lpInBuffer => 0x011b3ee8 nInBufferSize => 0x00000028 lpOutBuffer => 0x011b3ee8 nOutBufferSize => 0x00001000 lpBytesReturned => 0x013a7f98 lpOverlapped => 0x77e466e0	FAILURE		
03:43:17:807	ReadFile	hFile => 0x000007e8 nNumberOfBytesToRead => 848	SUCCESS		
03:43:17:807	CreateFileW	lpFileName => C:\Documents and Settings\sand\Application Data\Antivirus Protection\IcoActivate.ico dwDesiredAccess => GENERIC_WRITE	SUCCESS	0x0000074c	
03:43:17:807	WriteFile	hFile => 0x00000007 nNumberOfBytesToWrite => 12	SUCCESS		
03:43:17:807	WriteFile	hFile => 0x00000007 nNumberOfBytesToWrite => 18	SUCCESS		
03:43:17:807	WriteFile	hFile => 0x0000074c nNumberOfBytesToWrite => 894	SUCCESS		
03:43:17:807	WriteFile	hFile => 0x00000007 nNumberOfBytesToWrite => 2	SUCCESS		
03:43:17:807	CreateFileW	lpFileName => C:\Documents and Settings\sand\Application Data\Antivirus Protection\IcoHelp.ico dwDesiredAccess => GENERIC_WRITE	SUCCESS	0x0000074c	
03:43:17:827	WriteFile	hFile => 0x00000007 nNumberOfBytesToWrite => 12	SUCCESS		
03:43:17:827	WriteFile	hFile => 0x00000007 nNumberOfBytesToWrite => 11	SUCCESS		
03:43:17:827	WriteFile	hFile => 0x0000074c nNumberOfBytesToWrite => 894	SUCCESS		
03:43:17:847	WriteFile	hFile => 0x00000007 nNumberOfBytesToWrite => 2	SUCCESS		
03:43:17:847	CreateFileW	lpFileName => C:\Documents and Settings\sand\Application Data\Antivirus Protection\IcoUninstall.ico dwDesiredAccess => GENERIC_WRITE	SUCCESS	0x0000074c	
03:43:17:847	WriteFile	hFile => 0x00000007 nNumberOfBytesToWrite => 12	SUCCESS		
03:43:17:847	WriteFile	hFile => 0x00000007 nNumberOfBytesToWrite => 16	SUCCESS		

sub_40157A: No breakpoint!
Command "MakeAscii" failed

IDC

AU: idle Down Disk: 40GB

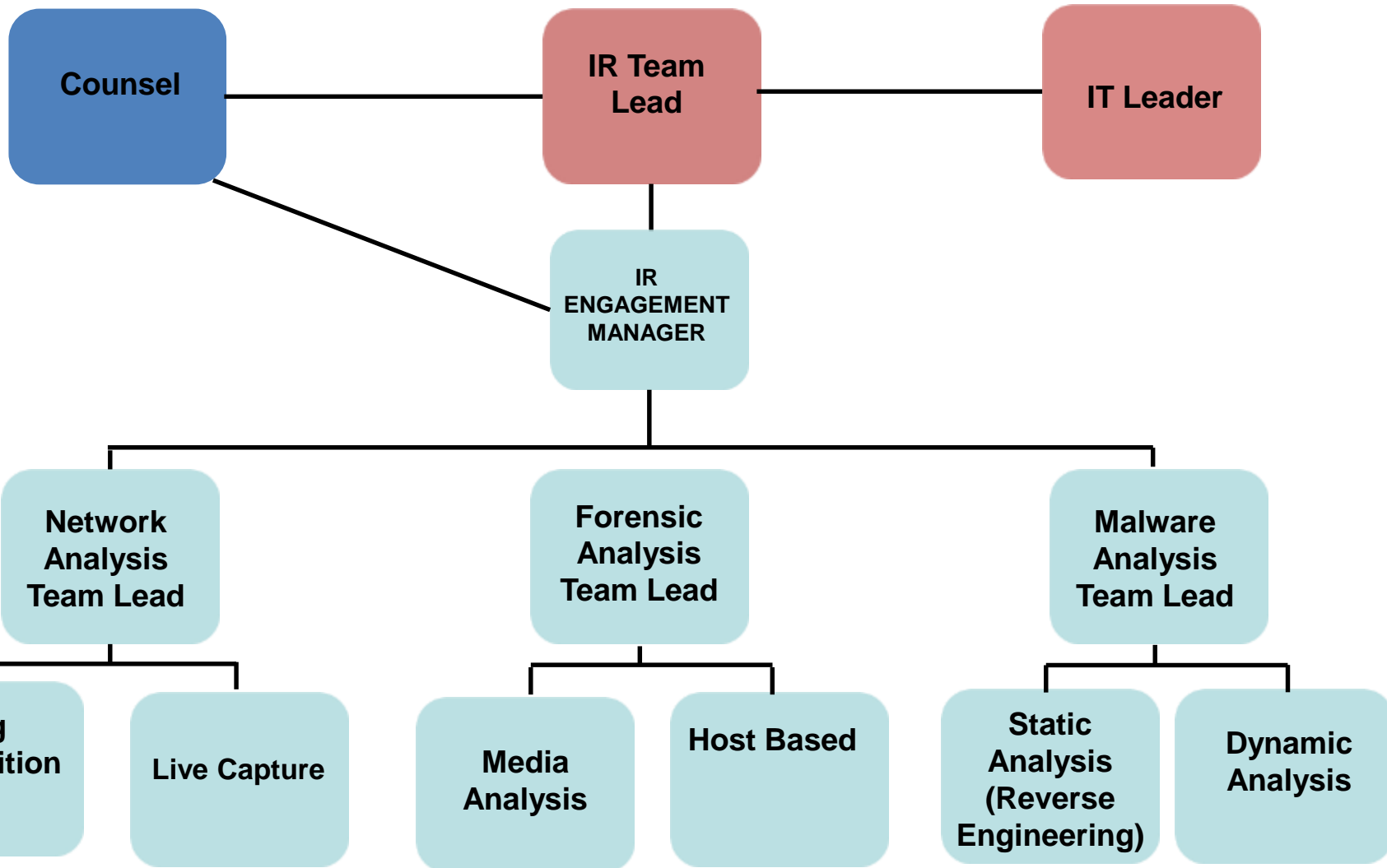
Scan hosts for Indicators of Compromise (“IOCs”)



LARGE SCALE ONSITE RESPONSE



TEAM APPROACH



THANK YOU

Randy V. Sabett, J.D., CISSP
Vice Chair, Privacy & Data Protection
Cooley LLP
1299 Pennsylvania Avenue, NW
Suite 700
(enter from 12th and E Streets)
Washington, DC 20004-2400
Direct: +1 202 728 7090
Cell: +1 202 257 7807
Email: rsabett@cooley.com
www.cooley.com
Bio: www.cooley.com/rsabett
Practice: www.cooley.com/privacy

Kenneth A. Mendelson, CISSP, CIPP
Managing Director
Stroz Friedberg
1150 Connecticut Avenue, NW
Suite 700
Washington, DC 20036
Direct: +1 202 464 5802
Cell: +1 202 415 0263
Email: kmendelson@strozfriedberg.com
www.strozfriedberg.com
Bio:
http://www.strozfriedberg.com/category/professionals?professional_bio_id=5