Investigating and Prosecuting Cybercrime
– Enter the Law Enforcement Trenches

Post-Conference Summary

Edward J. McAndrew
mcandrew@ballardspahr.com

Brian Coleman
Brian.coleman@pfizer.com

Melia Kelly
Melia.kelly@unitedlex.com
# Table of Contents

INTRODUCTION ..................................................................................................................... 3  
LAB SUMMARY ..................................................................................................................... 3  
   Key Takeaways .................................................................................................................. 4  
   Lessons Learned ............................................................................................................. 8  
   Some Resources .............................................................................................................. 8  

Introduction

Thank you for joining us in the law enforcement trenches to learn more about how cyber incident response moves from conference rooms and security operations centers to grand jury and courtrooms. We hope that your time with us, and at the 2017 RSA Conference overall, was educational and motivating. We especially hope that you walked out of our Lab with a sense of what it’s like for law enforcement professionals to assemble “the story” of a cybercrime spree into a case that is provable in a courtroom. As more cybercrime incidents end up in courtrooms over questions of both criminal liability for the actors and civil/regulatory liability for the victims, responding to cyber incidents in a way that enables others to “tell the story” is becoming increasingly critical.

This summary recaps our Learning Lab, and highlights some of the key takeaways and lessons learned from our cyber incident response and subsequent grand jury investigation. Although two hours was hardly enough time to scratch the surface on what are often very long, complex investigations, we thought that each group did a terrific job of spotting issues and marshaling evidence in a way that would have supported the return of actual indictments in our case.

Thanks again for choosing to spend some of your RSAC day with us, and we hope to see you next year!

Ed McAndrew, Brian Coleman & Melia Kelly

Lab Summary

Our Learning Lab centered on a cyberattack on an international law firm. The course of criminal conduct moved from intrusion and exfiltration of sensitive data, to attempts to extort the firm into altering its business activity in two ways: (1) withdrawing from the representation of a major client in high profile litigation; and (2) firing personnel working on behalf of that client – followed by a public acknowledgement of these actions. The conduct then expanded to threats of identity theft, financial fraud and violence directed at firm members and their families. The crime spree culminated in the publication of the firm’s stolen data on Watonleaks, including over 30,000 entries including confidential client communications, litigation strategies, internal criminal investigation materials, client intellectual property and discovery materials from class action litigation.

During Part One, we responded to this ongoing cyber incident, while assuming the role of an internal or external incident responder. Some of our tasks included:

- Detecting malicious cyber activity directed at your organization’s infrastructure, data and personnel;
- Containing the activity while collecting relevant evidence;
- Mitigating future harm from the bad actors;
- Coordinating and cooperating with a federal law enforcement investigation;
- Notifying impacted internal and external parties.

During Part Two, we assumed the roles of federal prosecutors and FBI agents conducting a grand jury investigation of the crimes committed during Part One. During the grand jury investigation, we:

- Identified evidence sources and witnesses inside and outside of the victim law firm;
• Spotted and discussed critical issues that impacted the direction of the investigation;
• Evaluated future investigative steps;
• Decided which criminal charges to include in an indictment; and
• Selected the evidence to be used to support each element of each crime.

We capped the Lab off with each team providing an oral presentation summarizing each charge it chose to include in the indictment and how it would prove each charge in a courtroom using the available evidence.

Key Takeaways

Cyber Incidents Are Organic Events that Often Continue after Initial Victim Discovery

Organizations and individuals learn that they are victims of cybercrime in different ways and at different points in the course of criminal conduct. A number of reports conclude that over two-thirds of victims learn of a cyber incident targeting them from a third party – ranging from law enforcement to business partners, the media or others impacted by the cyber conduct. Many victims learn of an intrusion long after it began – and often while it remains ongoing. In our experience and based on current research, “dwell” times in excess of 200 days are not uncommon. These factors greatly complicate an organization’s response upon discovery of some (often incomplete and inaccurate) set of facts regarding an incident. Because cybercriminal conduct is often ongoing, there is often great potential to gather the types of evidence that can lead to attribution, apprehension and prosecution of the offenders. Although they are of highest priority, incident detection and ongoing threat mitigation therefore must be balanced with investigative needs in securing existing evidence and developing additional evidence that may be necessary to long-term neutralization of the threat. Early expansion of internal response teams beyond in-house Info Sec/Info Tech and legal teams to include outside investigators, lawyers and law enforcement agencies is crucial to maximizing the potential for successful prosecution or other neutralization of the threat actors.

Cyber Incidents Often Have Personal Dimensions to Them

All cybercrime is personal. The objectives of cyber actors may extend well beyond financial gain. Even where their ultimate objective is to steal organizational data or impact organizational functioning, cybercriminals target individuals for attack. Individual device users often serve as the attack vectors or initial point of compromise into organizational networks. They are also vital sentries in the daily battle to defend digital assets. Individuals connected to organizations also can be targeted in very personal ways – such as identity theft, extortion, threats, stalking, and even physical violence. The targeting can even extend to an individual’s loved ones or personal and professional networks.

Due to their central role in attacks, individual users are often key players in the detection, remediation and investigation of cyber incidents. Incident responders, investigators and employers must appreciate the various perspectives from which these individuals are impacted by their involvement in a cyber incident – professional, financial, emotional, psychological, interpersonal, physical.
Proactive Incident Response Planning Is Critical to Effective Response

Understanding the cyber threat landscape and developing a practical plan for responding to different types of cyber incidents is absolutely essential for all organizations. This process starts with periodic cyber risk assessments that can form the basis of an information security program. There are a variety of proactive planning steps that organizations of any size can take to mitigate the harm caused by a cyber incident. By identifying key digital assets and operations, sharing cyber threat information, implementing technical, administrative and physical controls, raising user awareness about cyber threats, and tracking attempted or successful cyber incidents, organizations can plan to respond to the myriad incidents they may face. Incident response planning should include identification of core and extended response team members, definitions of different types of incidents and escalation thresholds, outlines of major roles and responsibilities in different incident response scenarios, guidelines for documenting investigative steps and cataloging evidence; crafting of communications strategies for foreseeable incidents, digesting of legal notification obligations and potential liabilities, and blueprinting of dispute resolution strategies. Another paramount practice is shifting cyber risk through insurance policies.

Identify and monitor key digital assets

Before creating a cyber incident plan, an organization should inventory and prioritize protection for its data, assets, and services. To the extent feasible, data mapping and continuous monitoring for threat indicators and anomalous user behavior should be performed.

Have a plan of action

Creating established plans and procedures to address what steps need to be taken after an incident is discovered can help any organization limit the impact of an incident. This includes identifying who has lead responsibility for different elements of an organization’s cyber incident response; the ability to contact critical personnel (inside of the organization and at all critical business partners) at all times, including through uncompromised communications channels; pre-existing relationships with outside legal counsel, forensic investigators, crisis managers, law enforcement for easy scaling if necessary; knowing what mission critical data, networks or services should be prioritized for the greatest protection and how to preserve data related to the incident in a forensically sound manner; cataloging all legal rights and obligations that may be relevant to a particular type of incident, including obligations to notify impacted individuals/organizations, regulators and others. Be prepared for potential regulatory investigations and litigation on multiple fronts, and to actively cooperate with law enforcement agencies that may be able to apprehend and prosecute attackers.

Engage with law enforcement before an attack

Having a pre-existing relationship with federal law enforcement officials can help facilitate real-time interaction and assistance during an incident. It will also help establish a trusted relationship that cultivates bi-directional information sharing that is beneficial to both the organization and law enforcement. As law enforcement agencies get better at “putting hands on” attackers, the likelihood of victim involvement in criminal investigation and prosecution is increasing. Actively playing the role of victim in such proceedings may aid your incident response and defensive strategies on other fronts.
Stay informed about threats

An organization’s awareness of new or commonly exploited vulnerabilities and attack types can help it prioritize its security measures and educate its user base. There are an increasing number of organizations and outlets that share real-time intelligence on threats. For example, Information Sharing and Analysis Centers, which analyze cyber threat information, have been created in each sector of the critical infrastructure. Some centers also provide cybersecurity services.

Create a methodology for initial threat assessment and escalation

Once an attack or breach is identified, containment must be the initial goal. Containment requires and quick and accurate assessment of the nature and scope of the incident. It is also important to determine whether the incident was a malicious act or a technological glitch. The nature of the incident will determine the appropriate response, including what kind of internal/external assistance the organization will need and what type of damage and remedial efforts may be required. Guidelines for answering these initial, key questions should be developed, memorialized and communicated to team members in advance. These guidelines should be reinforced through incident exercises that simulate different types of incidents.

Capture the extent of the damage

Have a game plan for memorializing investigative steps and relevant internal and external communications. Create a mechanism for collecting and preserving all relevant data and devices, and interviewing relevant witnesses. The use of attorney-client and attorney work product privileges is essential to ensuring that your investigative findings are not used against you by regulators and in courts. Therefore, to the greatest extent possible and practicable, ensure that investigative steps are undertaken at the direction of legal counsel and for the purpose of providing legal advice to the organization.

Take steps to minimize additional damage

An organization should articulate the broad strokes of a threat mitigation playbook that accounts for technical, administrative and physical issues that it may experience during different types of incidents. In addition to IT and security steps, this can include human resources planning, communications strategies, consumer and employee protection strategies, crisis management, disaster recovery/continuity of operations planning, as well as internal investigation and litigation strategies. Incorporate the lessons learned from each new cyber incident that your organization experiences to continually improve your cyber defenses and response strategies.

Grand Jury Investigations and Resulting Prosecutions Require Significant Victim Involvement

A federal grand jury is comprised of 23 qualified U.S. citizens. The function of the grand jury is to investigate possible criminal violations of the federal laws and to return indictments against culpable persons where there is probable cause to believe that a violation has occurred. In performing this function, "the grand jury is to inquire into all information that might possibly bear on its investigation until it has identified an offense or has satisfied itself that none has occurred." Grand jury investigations are led by federal prosecutors, who present witness testimony and evidence gathered during criminal investigations. These prosecutors have the power to subpoena witnesses and many other types of evidence in the name of the grand jury. They also present other types of evidence gathered by law enforcement agencies outside of the grand jury context, including physical and digital evidence and witness statements.
Organizational victims and their personnel play a critical role in the successful investigation and prosecution of cybercrime. Prosecutors should only indict what they can prove beyond a reasonable doubt – the burden of proof at trial. Meeting this burden often requires investigation into cyber conduct over an extended period of time with evidence gathered from multiple sources. Many investigations last for months, if not years, and involve multiple victims. It is not uncommon for law enforcement agents to ask victims to allow certain cyber conduct to continue so:

- it can be observed and documented;
- additional, corroborating evidence can be developed;
- bad actors can be identified and located;
- additional victims can be identified;
- targets can be taken into custody and successfully prosecuted.

All efforts are made to balance the needs of an investigation against those of threat mitigation and preventing additional injury to victims.

Victim involvement can be multi-faceted. A victimized organization’s network and devices are part of a digital crime scene that is often continuing to evolve as the conduct progresses. Victims are often asked to provide digital evidence of the cyber conduct in the form of preserved data and access to networks, devices and “server-side” data that are still active. Common types of evidence include log files and other system data establishing particular activities on devices or networks; internal or external communications with relevant individuals; indicators of compromise; copies of impacted data; testimony from pertinent employees or other users; use of digital assets or employees as part of the ongoing undercover investigation; analysis of stolen data that has been recovered; and valuation of losses caused by the criminal conduct.

Victim involvement can begin very early in the investigative process – often before any evidence is even presented to a grand jury. That involvement can continue through the indictment, pre-trial, trial and appellate phases of a case. It may carry over to related criminal cases or to civil litigation concerning asset recovery, seizure and forfeiture of ill-gotten proceeds obtained by bad actors, or liability of various parties involved in the incident as perpetrator or victim. It can include public testimony and evidence about the crimes and their impact on victims. It often requires the personal involvement of individuals within an organization over an extended period of time. For many businesses, it may be their (and their employees’) first exposure to the criminal justice process – and to cyber threat actors.

There are many benefits to victim cooperation in criminal investigations and prosecution. First, more cybercriminals need to be held accountable for their crimes. Victims are critical participants in holding them accountable. Second, participation in the criminal justice process may aid a victim in mitigating its liability before regulatory agencies or in civil matters. It also sends a message to the cybercriminal community that your organization is not a soft target. Third, with information provided by the government, victims can gain much greater insight into threat actors and cyber risk. As a result, they can better protect themselves going forward. Fourth, cyber incidents are often not the equivalent of spilled milk or a bad bucket list item. Even where an organization succeeds in containing a particular incident, the bad guys are not going to go away for long – and other bad guys are right around the corner. Successful investigation, neutralization and prosecution can have a much greater long-term impact on organizational cybersecurity.
Lessons Learned

1. Immediately ensure that your organization has an up-to-date cyber incident response plan for all foreseeable risks.

2. Evaluate what you would do if personally targeted for cyber-facilitated crime.

3. Include planning for extended involvement with law enforcement agencies in your organizational and personal cyber incident response plans.

4. Pay close attention to evolving cybersecurity threats and revise organizational and personal cyber incident response plans accordingly.

5. Integrate cyber and physical security at work and at home.

6. Establish relationships with key law enforcement and external incident responders now.

7. Continue to attend key security conferences to stay abreast on top security threats.

8. Conduct drills involving multiple departments (corporate communications, legal, family members, etc.) to test your incident response plans.

9. Spread the word about the necessity of cybersecurity.

Some Resources


https://www.cisecurity.org/critical-controls.cfm
Delaware Supreme Court Commission on Law & Technology

Legal Cloud Computing Association, Cloud Security Standards for Law Firms
http://www.legalcloudcomputingassociation.org/standards/#section1
Investigating and Prosecuting Cybercrime – Enter the Law Enforcement Trenches

FACILITATORS:

**Edward J. McAndrew**
Partner & Chair, Privacy & Data Security Group
Ballard Spahr LLP

**Brian Coleman**
Senior Manager, Global Information Security & Digital Forensics
Pfizer

**Melia Kelley**
Managing Consultant
Cyber Risk Solutions Practice
United Lex Corp.
Agenda for Today’s Lab – Phase One

- Respond to an Ongoing Cyber Incident.
  - Use information you learn to:
    - Detect malicious cyber activity directed at your organization’s infrastructure, data and personnel;
    - Contain the activity while collecting relevant evidence;
    - Mitigate future harm from the bad actors;
    - Coordinate and cooperate with law enforcement investigation;
    - Notify impacted internal and external parties.

- Focus on different roles and responsibilities of team members:
  - Technical – IT/Info Security
  - Legal
  - Compliance & Risk Management
  - Operations – Impacted business units, human resources, security
  - Communications
Agenda for Today’s Lab – Phase Two

- Work as prosecutors, law enforcement agents and senior members of victim organizations to investigate the crimes and prosecute the offenders.
  - Identify evidence sources and witnesses within the organization.
  - Identify evidence sources and witnesses outside of the organization.
  - Use information you learn to:
    - Spot critical issues that impact the direction of the investigation
    - Evaluate future investigative steps
    - Decide which charges to include in an indictment
    - Decide which evidence to present to the grand jury
Agenda for Today’s Lab – Phase Two

- Prepare a short opening statement to the grand jury in support of the charges that you include in a proposed indictment.
- Identify some of the key pieces of evidence you would use to prove each element of each charged crime.
- Identify other types of evidence you would seek and other areas for further investigation.
Schedule

- 4:00 – 4:30 – Cyber Incident Small Group Response
- 4:30 – 4:40 – Group Discussion of Incident Response Key Points
- 4:40 – 5:20 – Law Enforcement Investigation and Grand Jury Preparation
- 5:20 – 6:00 – Grand Jury Presentations & Group Discussion
BigLaw LLP is a global law firm employing over 3,000 lawyers in more than 30 offices around the world. BigLaw’s U.S. headquarters is in San Francisco, CA – where its global chairperson, COO, CFO, CISO, CPO and communications team are located.

On February 15, 2017, at about 4:03 p.m., the computer screens of the firm leaders went blank and their world changed . . .
What’s a Cyber Incident?

- An adverse event that threatens the confidentiality, integrity, or availability of information assets, information systems, and the networks that deliver the information.

Responding to a Cyber Incident

- Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.
- Contain the malicious activity and stop any data loss, system disruption/destruction, physical threats.
- Collect and preserve data related to the incident.
- Evaluate whether you must or should notify internal and external parties, including law enforcement.
Internal Concerns

- Incident Confirmation and Notification
- Mitigation of Ongoing Incidents
- Attribution
- Information Sharing
- Threats of Dissemination
- Possible Business Disruption/Destruction
- Ancillary Business Concerns
Understanding the Cyber Incident

- Type of Attack
- Means of Access
- Data/Systems/Devices Subject to Exposure or Compromise
- Movements within Networks
- Individuals Involved
- Time Period of Incident
- Current Status of Data/Systems/Devices
- Attribution, Mitigation and Remediation
Governmental Concerns

- Severity of Attack
- Organizational Resiliency
- Impact on Industry Sectors
- Economic and National Security Implications
- Pervasiveness and Connectedness of Incident(s)
- Attribution
- Evidence Gathering and Victim Cooperation
- Potential for Success of Different Governmental Tools
Part 1 – The Threat and Extortionate Demand
The Threat

- BigLaw’s leaders’ computer screens contain the following:
  - Unknown person(s) have gained access to BigLaw’s internal network and attorney devices and have exfiltrated confidential and highly sensitive firm and client data.
  - They will disseminate this data to Internet and media outlets, unless BigLaw:
    - Withdraws from representing SpaceCar Corp., an autonomous automobile manufacturer, in hundreds of class action cases across the country. These cases allege product liability claims based on faulty security in SpaceCar autonomous vehicles that have been involved in numerous fatal crashes.
    - Fires a former U.S. Senator and his team of lawyers in the firm’s Washington, D.C. office who have been lobbying on behalf of SpaceCar to oppose the creation of autonomous automobile safety regulations.
    - Publicly acknowledges these actions and apologizes for representing SpaceCar in courts and on Capitol Hill while knowing of the significant risks posed by its autonomous vehicles.
!!! IMPORTANT INFORMATION !!!

Your data has been encrypted with RSA-2048 and AES-128 ciphers.

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

As an extra precaution, we have copied your data to our secret location. This information has to do with various aspects of the business and it could potentially be of interest to regulatory bodies, your competitors, partners, company employees, general population, etc. Unless we can come to some kind of an agreement or if we get no reply all of the information in our possession will be published online.

To get your data back you MUST do the following:

Withdraw from representing SpaceCar Corp.
Fire former Senator BigWig and his team of lawyers
Publicly acknowledge these actions and apologize for representing SpaceCar in courts and on Capitol Hill

This must be done within 48 Hours. We will be watching you.
Group Discussion – Threat Response

- Who do you notify?
- What questions do you ask?
- Who decides whether to declare an “incident”?
- How is the decision made?
- How do you classify the incident? – Risk Level
- Do you convene a meeting of the IR Team?
- Who is on the team?
CSIRT Initial Response

Internal IT/IS resources deployed
Immediately determine what action, if any, will eliminate the problem or minimize the damage
Gather and document the details associated with the incident within the Incident Response System:
• the date and time of the incident;
• business line or location affected by the incident;
• description of the incident;
• mitigation plan actions;
• the parties affected (number of employees, number of clients, and number of third parties);
• the types of information involved;
• the geographic region, country or state where the information originated from;
• additional information (specific to type of incident)
Classify and categorize the incident based on reported details
Assign "Incident Manager" based on categorization and risk assigned
Initiate *internal* communications (Sponsors, Standing Members, Incident Manager)
4 Hours – Detect, Mitigate, Report and Assign

• How do internal communications take place?

• Who will be included?

• Will a meeting be called? Email? Phone?

• Where does the meeting occur?

• Who provides the initial report on facts? What is included?

• What is agenda for first meeting?

• What are investigative objectives coming out of these steps?

• When should the executive team be briefed?
Group Discussion – Call Law Enforcement?

QUESTIONS:

• Which law enforcement agency do you notify?
• What information do you provide?
• Do you provide network/device access?
• Do you re-classify the incident? – Risk Level
Part 2 – Internal Investigation of the Hack and the Data Theft
Group Discussion

- Who do you notify?
- What are the immediate next steps?
- How will you identify the compromised host?
- Will you preserve and collect the evidence?
  - What software and/or hardware will you use?
  - In what order will you collect the evidence?
  - “Best Evidence” and “Working Copy”
- Who is taking notes?
Investigative Action Plan

- Develop Compromised Host Evidence Investigative Action Plan
  - Who has access to the system in question?
  - Internal Resources
    - Will the team perform its own analysis?
    - What programs and techniques will be used?
    - What data is prioritized for analysis?
  - Forensics/Incident Response Vendor
    - Defensibility of process
    - Assert attorney client privilege or work product protection
    - Effectiveness of process
Group Discussion

- Identify/preserve/collection the data associated with the potentially compromised host.
  - Logs (e.g. access logs, host event logs, firewall logs, etc.)
  - RAM
  - Backups

- With regard to the general preservation of evidence, the most volatile sources of data should be collected first, and prioritize sources based on a descending order of volatility.

- Monitor event logs and look for factors resembling illegal activity and/or exfiltration.

- Consider steps to terminate or block illegal traffic/activity.

- Consider steps to determine if scope and scale is broader than the single identified server.

- Additional forensic techniques and processes are dependent on the circumstances, technology involved, and infrastructure involved.

- Consider identities associated with the host to be compromised and general impact.
Analysis of Compromised System

- Document real-time decisions and discussions from group.
- Perform Forensic Analysis
  - What was exposed?
  - What was compromised?
  - When did the compromise start?
  - Is the compromise still on-going?
  - How did the compromise occur?
  - What accounts were associated with this issue?
  - Who is the main subject? (Insider, Competitor, Third Party)
  - Where has the data been exfiltrated to?
I. Executive Summary

This report was created for BigLaw LLP (“BigLaw”) for use in a Ransomware investigation. UnitedLex was hired to forensically acquire one Seagate Barracuda 500GB 3.5” desktop hard drive (Serial# Z6EES7R4) and examine it for origination of suspected malware. The hard drive was delivered to UnitedLex’s Overland Park headquarters for imaging in the Cyber Forensics Lab.

II. Analysis

A. Seagate Barracuda 500GB 3.5” desktop hard drive
   1. Using various tools and techniques, the hard drive was examined for evidence of when and how the malware originated. Additionally, the drive was examined for evidence of exfiltration of data.

B. Malware
   1. The malware underwent multiple tests to determine its capabilities. Testing included open source research, sandboxing, and static analysis.
   2. Two pieces of malware were identified and analyzed.
III. Summary

The malware origination was confirmed to come from a USB drive. The initial infection malware was a file called “ClickMe.exe”. When clicked, this executable immediately begins running in the background and remains in a listening state until a remote attacker opens a meterpreter shell. Once connected via the shell the attacker would have remote access and could execute commands on the victim machine.

Analysis indicates that the attacker performed multiple actions, including downloading a secondary piece of malware. This secondary malware is a relatively new ransomware variant that encrypts certain file types and communicates to an IP that geolocates to Maryland. No decryption method is currently available for the encrypted files.

Neither of the malware pieces have automatic exfiltration built into the code. However, the attacker would have had the ability to manually perform exfiltration using the known meterpreter session. If historical network data such as full packet captures is available for this timeframe a positive identification of exfiltration may be found.
Stolen Employment and IT Data

<table>
<thead>
<tr>
<th>Position Information</th>
<th>Data Cut</th>
<th>Base Salary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incumbent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>n</td>
<td>10th</td>
</tr>
<tr>
<td>115</td>
<td>22016 Animation Art Director</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>116</td>
<td>24024 Senior / Lead Visual Development Artist</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>117</td>
<td>24025 Visual Development Artist</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>118</td>
<td>24027 Visual Development Artist</td>
<td>Southern California - Animation and Visual Effects</td>
</tr>
<tr>
<td>119</td>
<td>24026 Associate Visual Development Artist</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>120</td>
<td>28016 Model Supervisor</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>121</td>
<td>28024 Senior / Lead Modeler</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>122</td>
<td>28025 Modeler</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>123</td>
<td>28023 Layout Supervisor</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>124</td>
<td>28024 Senior / Lead Layout Artist</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>125</td>
<td>28025 Layout Artist</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>126</td>
<td>30012 Head of Character Animation</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>127</td>
<td>30016 Animation Supervisor</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>128</td>
<td>30024 Senior / Lead Animator</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>129</td>
<td>28026 Animator</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>130</td>
<td>30026 Associate Animator</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>131</td>
<td>40012 CG Supervisor</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>132</td>
<td>41016 Character Set Up / Rigging Supervisor</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
<tr>
<td>133</td>
<td>41024 Senior / Lead Character Set Up / Rigging</td>
<td>All Incumbents - Animation and Visual Effects</td>
</tr>
</tbody>
</table>
Part 3 – Personal Threats
The Threat

At 11:59 p.m., on February 15, BigLaw’s Chairperson and CISO receive emails at their personal Yahoo accounts and text messages on their personal phones.

The messages contain personalized threats to solicit acts of identity theft and violence against 25 employees working on the SpaceCar class actions and lobbying campaign (and their spouses and children) if the demands are not met.

Attached to the emails are data files containing the following information about the targeted employees:

- Name, home, work/school addresses, SSNs, DOBs, photographs of employees and some spouses and minor children;
- Calendar entries for employees for February 16, 2017 (some including personal appointments for the employee, spouse or children);
- Bank statements for each employee from the account used for direct deposits from BigLaw;
- 401K account information for each employee; and
- The following photograph:
None of You Are Safe . . .
Part 4 – The Data Dump
Attorney and Firm Leaders’ Emails and Data Files -- 30,000 data files uploaded to WantonLeaks

- Confidential communications with BigLaw’s top 15 clients
- Litigation strategies and case evaluations for the SpaceCar class actions
- “email purge” directives in litigation matters for SpaceCar
- Foreign Corrupt Practices Act internal investigation materials relating to SpaceCar
- Materials relating to SpaceCar’s autonomous vehicle intellectual property
- Discovery materials from various intellectual property, securities, employment and product liability matters for SpaceCar
Attacks Targeting Individuals

Employees and FBI Agent Doxed

- Some employees (and FBI agents) receive threatening messages, by Internet posting, email and phone calls.

- Home addresses and pictures of Chairperson and CISO’s children are posted to a dark web forum at http://hell1s4chldn.onion.
The Grand Jury Investigation
Based in part on information provided by BigLaw, the FBI has identified a suspect ("ALBUS") who may have been involved in the attacks.

FBI obtains remote search warrant for one computer known to have been used to access a dump server for exfiltrated BigLaw data.

Seized data includes webcam photo of one suspect; Facebook, Yahoo and other accounts accessed from the computer; IP addresses used by the computer (including one used to access the dump server); and data files that appear to have been stolen from BigLaw.
Pen Trap & Trace/2703(d) Hybrid Order on Facebook account identified through remote search warrant produces:

- basic subscriber information, including an associated cell phone number
- data showing log-ins in the vicinity of BigLaw’s San Francisco headquarters
- Log-in IP address matching that used to access the dump server
ALBUS Visited BigLaw Headquarters

- GPS Search Warrant to cellphone service provider reveals that ALBUS’s cell phone visited the block of BigLaw’s headquarters nearly every day for a 2-week period in Jan/Feb.
- Data also reveals same residential location of cell phone every night.
- Public database check lists ALBUS as resident of home, and 2 Honda vehicles registered in his name to the address.
Picture Posted on Facebook Account Associated with ALBUS
Residential Search
Residential Search and Interview of ALBUS

- FBI Agents execute a residential SW at 0600, on March 1, 2017.
- ALBUS is the lone occupant of the house. His wife died in a head-on crash with a SpaceCar autonomous vehicle.
- Agents locate multiple weapons (assault rifles, shotguns, handguns, knives, and ammunition) throughout the house. A number of the firearms are loaded and located in common rooms and bedrooms.
Interview of ALBUS

- ALBUS agrees to speak with the agents.
  - ALBUS confirms his cell phone number and Facebook account and posting of bullets photo. ALBUS is an officer for a private secretive security service, and a gun enthusiast.
  - ALBUS confirms that he knows BigLaw represents SpaceCar in the product liability class actions referenced in the initial threat BigLaw received.
  - ALBUS denies any involvement in the cyberattack on BigLaw or threats to individuals.
Search Photo of “Computer Room” in ALBUS’s Residence
ALBUS’s iPhone and Numerous Devices Are Encrypted
Unlocking Smart Phones

### IN THE UNITED STATES DISTRICT COURT

**FOR** ____________

**APPLICATION**

**Filed Under Seal**

---

**INTRODUCTION**

The United States of America, by and through ________, United States Attorney, and ____ Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring Google, Inc. (“Google”) to assist in the execution of a federal search warrant by bypassing the lock screen of an Android device, specifically, an [DEVICE NAME].

**FACTS**

The [AGENCY] currently has in its possession an Android device [PICK ONE][that was seized pursuant to a search warrant issued by this Court] (that is the subject of a search warrant issued by this Court). Initial inspection of the Android device reveals that it is locked.
Cars Seized in BigLaw Parking Garage and at ALBUS’s Residence
Results from FBI Forensic Analysis of Decrypted Laptop
Malware Analysis
# Stealing Log-in Credentials

![Image of an Excel spreadsheet showing stolen login credentials](image-url)

<table>
<thead>
<tr>
<th>Email</th>
<th>Password</th>
<th>SteamAccount</th>
<th>Project</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:testronicity1@hotmail.co.uk">testronicity1@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity1@hotmail.co.uk">testronicity1@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity2@hotmail.co.uk">testronicity2@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity2@hotmail.co.uk">testronicity2@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity3@hotmail.co.uk">testronicity3@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity3@hotmail.co.uk">testronicity3@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity4@hotmail.co.uk">testronicity4@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity4@hotmail.co.uk">testronicity4@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity5@hotmail.co.uk">testronicity5@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity5@hotmail.co.uk">testronicity5@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity6@hotmail.co.uk">testronicity6@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity6@hotmail.co.uk">testronicity6@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity7@hotmail.co.uk">testronicity7@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity7@hotmail.co.uk">testronicity7@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity8@hotmail.co.uk">testronicity8@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity8@hotmail.co.uk">testronicity8@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity9@hotmail.co.uk">testronicity9@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity9@hotmail.co.uk">testronicity9@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity10@hotmail.co.uk">testronicity10@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity10@hotmail.co.uk">testronicity10@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity11@hotmail.co.uk">testronicity11@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity11@hotmail.co.uk">testronicity11@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity12@hotmail.co.uk">testronicity12@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity12@hotmail.co.uk">testronicity12@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity13@hotmail.co.uk">testronicity13@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity13@hotmail.co.uk">testronicity13@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity14@hotmail.co.uk">testronicity14@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity14@hotmail.co.uk">testronicity14@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
<tr>
<td><a href="mailto:testronicity15@hotmail.co.uk">testronicity15@hotmail.co.uk</a></td>
<td>HitmanES01</td>
<td><a href="mailto:testronicity15@hotmail.co.uk">testronicity15@hotmail.co.uk</a></td>
<td>Tomb Raider</td>
</tr>
</tbody>
</table>
Moving Laterally to Find Additional Credentials
Root Access
Compromising Personal & Professional Accounts
Stealing Data from BigLaw Server
Download History of .rar files related to BigLaw

<table>
<thead>
<tr>
<th>Download History of .rar files related to BigLaw</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gear_Xenon_[2011-02-18_09.39]_[INTSkul].part09.rar</td>
</tr>
<tr>
<td>Gear_Xenon_[2011-02-18_09.39]_[INTSkul].part08.rar</td>
</tr>
<tr>
<td>Gear_Xenon_[2011-02-18_09.39]_[INTSkul].part07.rar</td>
</tr>
<tr>
<td>Gear_Xenon_[2011-02-18_09.39]_[INTSkul].part06.rar</td>
</tr>
<tr>
<td>Gear_Xenon_[2011-02-18_09.39]_[INTSkul].part05.rar</td>
</tr>
<tr>
<td>Gear_Xenon_[2011-02-18_09.39]_[INTSkul].part03.rar</td>
</tr>
</tbody>
</table>

To return to your computer, press Control-C.
Stealing Financial Account Information
Monitoring Investigations

Re: intrusion data

Sent: Friday, July 15, 2011 6:21 PM

To: [Redacted]
Cc: [Redacted]

I'm out of town at the moment. We have syslogs, but they rotate after a week. I was primarily seeing Russia and a couple of places in South America. I'm adding W... so he can assist.

Sent from my mobile device. Please excuse typos.

On Jul 15, 2011, at 9:50 PM, [Redacted] wrote:
> S, was there any additional info on...? or other software leaving... servers as a result of malware?
> Also, are you able to provide any DNS, server logs, etc. with regard to unknown remote connections?
> Regards,
Surveillance Video of CISO’s Residence
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/6/2013</td>
<td>11:51:45 PM</td>
<td><a href="http://www.google.com/search?q=catholic">Link to Google search</a></td>
</tr>
<tr>
<td>2/6/2013</td>
<td>11:50:02 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/6/2013</td>
<td>11:48:02 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic prayer</a></td>
</tr>
<tr>
<td>2/6/2013</td>
<td>11:48:18 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic Online</a></td>
</tr>
<tr>
<td>2/6/2013</td>
<td>11:48:36 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/6/2013</td>
<td>11:44:35 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/6/2013</td>
<td>11:42:21 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/6/2013</td>
<td>11:42:39 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/6/2013</td>
<td>11:42:20 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/6/2013</td>
<td>10:29:38 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/5/2013</td>
<td>10:25:09 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/5/2013</td>
<td>10:24:58 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/5/2013</td>
<td>1:43:38 AM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/5/2013</td>
<td>1:43:38 PM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/5/2013</td>
<td>1:43:10 AM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/5/2013</td>
<td>1:42:35 AM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
<tr>
<td>2/5/2013</td>
<td>1:42:15 AM</td>
<td><a href="http://www.catholic.org/prayers">Link to Catholic site</a></td>
</tr>
</tbody>
</table>
Shooting Photo in Threat Email Is from a Real Case

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

UNITED STATES OF AMERICA,

Plaintiff,

v.

DAVID THOMAS MATUSIEWICZ,
LENORE MATUSIEWICZ, and
AMY GONZALEZ,

 Defendants.

Criminal Action No. 13-959-WWV
(Sealed)

SEALLED

INDICTMENT

The Grand Jury for the District of Delaware charges that:

1. GENERAL ALLEGATIONS COMMON TO ALL COUNTS
   1. DAVID THOMAS MATUSIEWICZ and AMY GONZALEZ are the biological children of THOMAS MATUSIEWICZ and LENORE MATUSIEWICZ (hereinafter the "MATUSIEWICZ Family").
   2. DAVID THOMAS MATUSIEWICZ and Christine Belford were married on or about October 13, 2001. They divorced on or about November 30, 2006.
   3. During their five-year marriage, DAVID THOMAS MATUSIEWICZ and Christine Belford had three children, who will be referred to throughout this indictment as Jane Doe 1, 2 and 3. Christine Belford also had a child from a previous marriage, who will be referred to as Jane Doe 4.
   4. During and after the divorce proceedings, DAVID THOMAS MATUSIEWICZ and Christine Belford engaged in a custody dispute regarding Jane Doe 1, 2 and 3.
The Grand Jury & Charging Decisions
Unauthorized Computer Access
(18 U.S.C. § 1030(a)(2) (B) & (C))

1. Defendant accessed a computer without authorization or exceeded authorized access to a computer;

2. Defendant thereby obtained any of the following:

   (C) information from any protected computer if the conduct involved an interstate or foreign communication; and

3. Defendant did so intentionally.

“Protected computer” – any computer connected to the Internet
Identity Theft (18 U.S.C. § 1028(a)(7))

1. Defendant knowingly used, without lawful authority, a means of identification of another person;

2. Defendant so acted with the intent to commit an unlawful activity that constitutes a violation of Federal law; and

3. The use was in or affecting interstate commerce.
Digital Threats
18 U.S.C. § 875(c)

1. Defendant transmitted in interstate or foreign commerce;
2. Any communication containing any threat to kidnap or injure any person; and
3. Defendant had the purpose of issuing a threat or the knowledge that the communication would be viewed as a threat.
Cyberstalking
18 U.S.C. § 2261A(2)

1. Defendant used the mail, an interactive computer service, or any other facility of interstate commerce;

2. To engage in a course of conduct with the intent to kill, injure, harass or place under surveillance with the intent to kill, injure, harass, or intimidate, or cause substantial emotional distress to another person; and

3. As a result of that course of conduct, that person experienced substantial emotional distress or was placed in reasonable fear of the death of, or serious injury to, herself or a member of her immediate family, her spouse or intimate partner.
First Amendment Implications of Speech-related Cybercrime

Certain “well-defined and narrowly limited classes of speech” are not protected by the First Amendment:

- Defamation
- Fraud
- Incitement
- Obscenity/Child Pornography
- Speech integral to criminal conduct
- True threats
Next week you should:
- Ensure that your organization has an up-to-date cyber incident response plan for all foreseeable risks.
- Evaluate what you would do if personally targeted for cyber-facilitated crime.

Within 3 months, you should:
- Create/revise organizational and personal cyber incident response plans.
- Integrate cyber and physical security.
- Establish relationships with key law enforcement and external incident responders.

Within six months you should:
- Attend key security conferences to stay abreast on top security threats.
- Conduct drills involving multiple departments (corporate communications, legal, etc.) to test your incident response plan.