ETRAC Presentation ECCN 4E001.c – "Intrusion Software" Technology

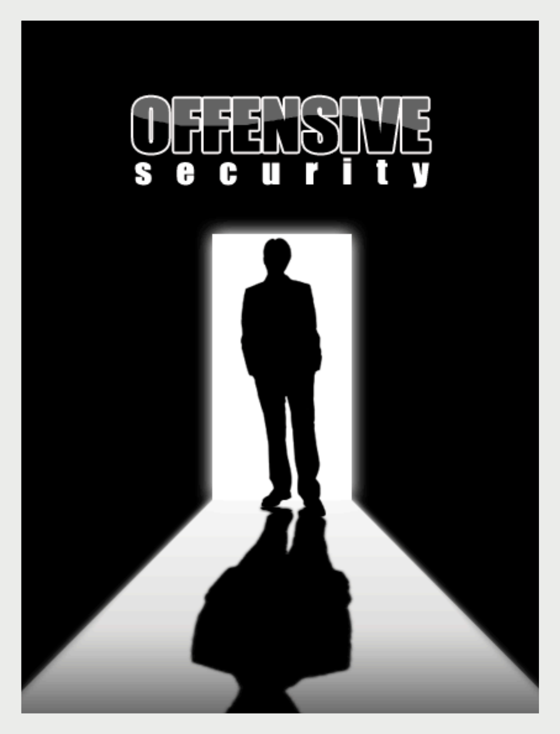
OFFENSIVE® security

www.offensive-security.com

Jim O'Gorman, President
October 15, 2015

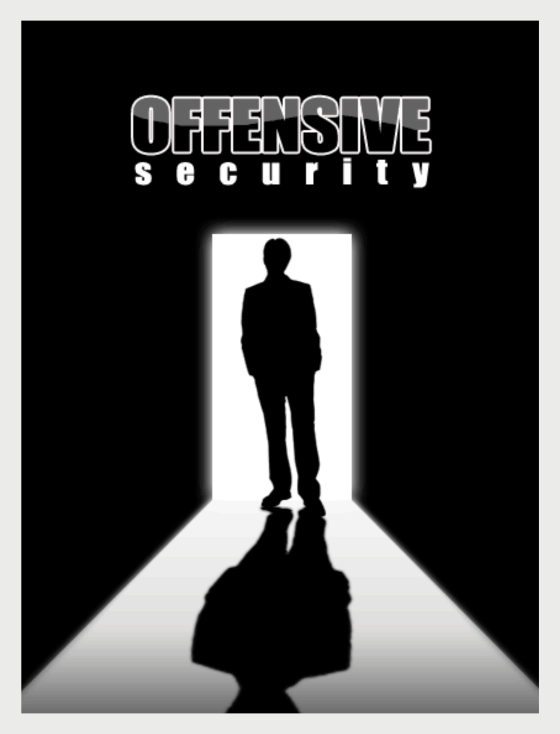
OFFENSIVE SECURITY - PROJECTS

- **KALI LINUX (PREVIOUSLY BACKTRACK LINUX)**
- INDUSTRY STANDARD OPEN SOURCE PENETRATION TESTING PLATFORM
- **EXPLOIT DB**
- COMPREHENSIVE ARCHIVE OF EXPLOITS, SHELLCODE, AND SECURITY PAPERS
- COMPRISING OVER 34,000 OPEN SOURCE EXPLOITS
- CVE COMPLIANT



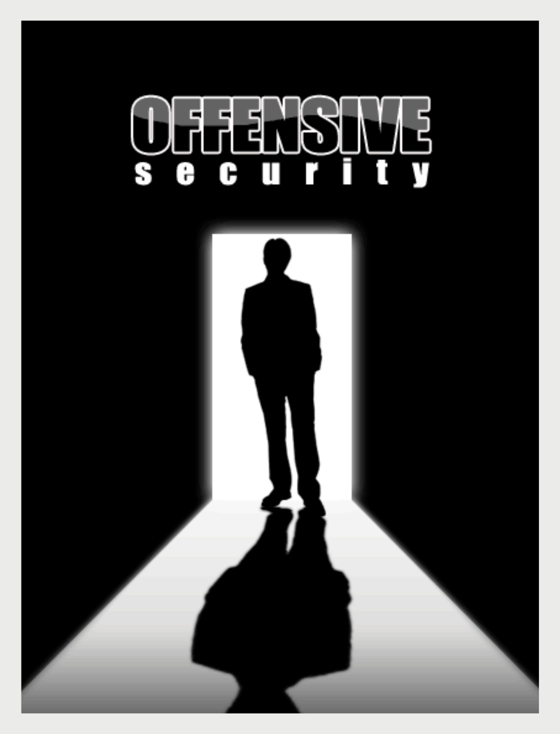
OFFENSIVE SECURITY - ABOUT

- FOUNDED IN 2007
- BASED ON THE BELIEF THAT THE ONLY WAY TO ACHIEVE SOUND DEFENSIVE SECURITY IS THROUGH AN OFFENSIVE APPROACH
- TRAININGS AND CERTIFICATIONS
- OSCP, OSCE, OSWP, OSWE, OSEE
- PWK, CTP, WIFU, AWE, AWAE



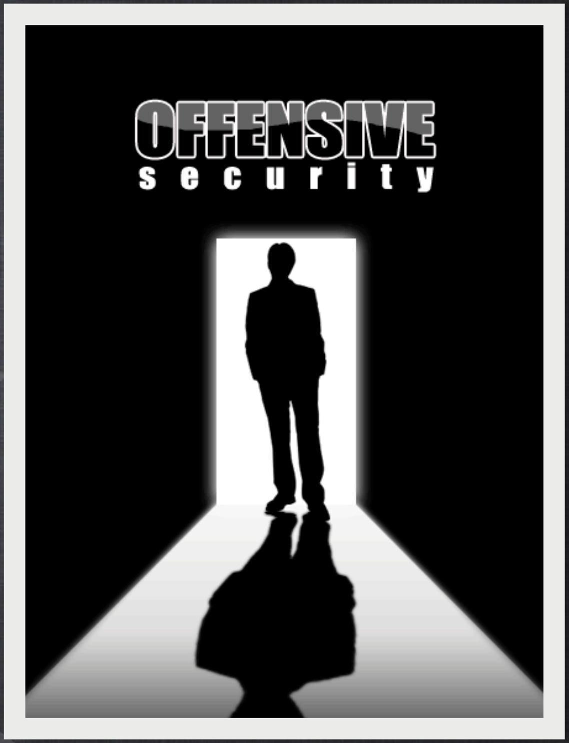
OFFENSIVE SECURITY - SERVICES

- PROVIDES HIGHLY ADVANCED, TEAM-BASED SECURITY ASSESSMENTS
- CLIENTS INCLUDE FORTUNE 100, FINANCIAL, MILITARY, LAW ENFORCEMENT, AND HEALTHCARE ORGANIZATIONS
- REAL WORLD, MAXIMUM IMPACT, EXTREMELY SKILLED AND TARGETED HACKER SIMULATION
- ACTIVELY DISCOVERING AND EXPLOITING VULNERABILITIES IN SOFTWARE SUCH AS SYMANTEC, CA, HP, MICROSOFT OFFICE, ETC.



OFFENSIVE SECURITY - OVERALL

- SPEAKING STRICTLY ON BEHALF OF OFFENSIVE SECURITY
- HAVE ENGAGED WITH VARIOUS OTHER ORGANIZATIONS AND INDIVIDUALS FROM THE HACKING COMMUNITY FOR INPUT
- NOT ENOUGH INPUT HAS BEEN SOLICITED FROM THE HACKING/INFORMATION SECURITY COMMUNITY



PROPOSED TECHNOLOGY CONTROLS

PROPOSED ECCN 4E001.C

- "TECHNOLOGY" "REQUIRED" FOR THE "DEVELOPMENT" OF "INTRUSION SOFTWARE"
- "TECHNOLOGY": SPECIFIC INFORMATION NECESSARY FOR THE "DEVELOPMENT", "PRODUCTION", OR "USE" OF A PRODUCT. THE INFORMATION TAKES THE FORM OF 'TECHNICAL DATA' OR 'TECHNICAL ASSISTANCE'. 15 C.F.R. § 772.
- NOTE 1: "TECHNOLOGY" IS ALSO SPECIFIC INFORMATION NECESSARY FOR ANY OF THE FOLLOWING: OPERATION, INSTALLATION (INCLUDING ON-SITE INSTALLATION), MAINTENANCE (CHECKING), REPAIR, OVERHAUL, REFURBISHING, OR OTHER TERMS SPECIFIED IN ECCNS ON THE CCL THAT CONTROL "TECHNOLOGY." 15 C.F.R. § 772.
- 'TECHNICAL DATA' MAY TAKE FORMS SUCH AS BLUEPRINTS, PLANS, DIAGRAMS, MODELS, FORMULAE, TABLES, ENGINEERING DESIGNS AND SPECIFICATIONS, MANUALS AND INSTRUCTIONS WRITTEN OR RECORDED ON OTHER MEDIA OR DEVICES SUCH AS DISK, TAPE, READ ONLY MEMORIES. 15 C.F.R. § 772 (TECHNICAL NOTE).
- 'TECHNICAL ASSISTANCE' MAY TAKE FORMS SUCH AS INSTRUCTIONS, SKILLS, TRAINING, WORKING KNOWLEDGE, CONSULTING SERVICES. 'TECHNICAL ASSISTANCE' MAY INVOLVE TRANSFER OF 'TECHNICAL DATA'. 15 C.F.R. § 772 (TECHNICAL NOTE).

INTRUSION SOFTWARE

PROPOSED ECCN 4D004

- “SOFTWARE” “SPECIALLY DESIGNED” OR MODIFIED FOR THE GENERATION, OPERATION OR DELIVERY OF, OR COMMUNICATION WITH “INTRUSION SOFTWARE”.
- INTRUSION SOFTWARE. (CAT 4) “SOFTWARE” “SPECIALLY DESIGNED” OR MODIFIED TO AVOID DETECTION BY ‘MONITORING TOOLS,’ OR TO DEFEAT ‘PROTECTIVE COUNTERMEASURES,’ OF A COMPUTER OR NETWORK-CAPABLE DEVICE, AND PERFORMING ANY OF THE FOLLOWING:
- (A) THE EXTRACTION OF DATA OR INFORMATION, FROM A COMPUTER OR NETWORK-CAPABLE DEVICE, OR THE MODIFICATION OF SYSTEM OR USER DATA; OR
- (B) THE MODIFICATION OF THE STANDARD EXECUTION PATH OF A PROGRAM OR PROCESS IN ORDER TO ALLOW THE EXECUTIONS OF EXTERNALLY PROVIDED INSTRUCTIONS.

WHAT IS THE POLICY RATIONALE?

THE BAD CONDUCT IS ALREADY UNLAWFUL:

- COMPUTER FRAUD AND ABUSE ACT
- ELECTRONIC COMMUNICATIONS PRIVACY ACT
- DIGITAL MILLENNIUM COPYRIGHT ACT
- CYBER SECURITY ENHANCEMENT ACT
- IDENTITY THEFT ENFORCEMENT AND RESTITUTION ACT
- ECONOMIC ESPIONAGE ACT
- IP INFRINGEMENT
- TRESPASS, THEFT, ETC

ETRAC QUESTION #1

"IS IT POSSIBLE TO INTERPRET PROPOSED ECCN 4E001.C AND THE DEFINITION OF "INTRUSION SOFTWARE" IN SUCH A WAY THAT LEGITIMATE CYBERSECURITY RESEARCH WOULD NOT BE AFFECTED?":

- NO
- THE FUNDAMENTAL PROBLEM IS THAT THE DEFINITION OF "INTRUSION SOFTWARE" BEGINS TOO BROADLY, AND THEN TRIES TO EXCEPT WHAT IS CONSIDERED TO BE "LEGITIMATE" ITEMS
- THE "REGULATE BROADLY AND THEN MAKE EXCEPTIONS" FRAMEWORK IS UNWORKABLE IN A DYNAMIC TECHNOLOGY AREA

ETRAC QUESTION #1

ITEMS EXPLICITLY NOT COVERED:

HYPERVISORS (NOTE 1)

DEBUGGERS (NOTE 1)

SOFTWARE REVERSE ENGINEERING (SRE) TOOLS (NOTE 1)

DIGITAL RIGHTS MANAGEMENT (DRM) SOFTWARE (NOTE 1)

SOFTWARE DESIGNED TO BE INSTALLED BY MANUFACTURERS, ADMINISTRATORS, OR USERS, FOR THE PURPOSE OF ASSET TRACKING OR RECOVERY (NOTE 1)

EXPLOIT SAMPLES (FAQ #1)

EXPLOIT PROOF OF CONCEPTS (FAQ #1)

OTHER FORMS OF MALWARE (FAQ#1)

INFORMATION ON HOW TO SEARCH FOR, DISCOVER OR IDENTIFY A VULNERABILITY IN A SYSTEM, INCLUDING VULNERABILITY SCANNING (FAQ #4)

INFORMATION ABOUT A VULNERABILITY, INCLUDING THE CAUSES OF A VULNERABILITY (FAQ #4)

INFORMATION ON TESTING THE VULNERABILITY, INCLUDING 'FUZZING' OR OTHERWISE TRYING DIFFERENT INPUTS TO DETERMINE WHAT HAPPENS (FAQ #4)

INFORMATION ON ANALYZING THE EXECUTION OR FUNCTIONALITY OF PROGRAMS AND PROCESSES RUNNING ON A COMPUTER, INCLUDING DECOMPILING OR DISASSEMBLING CODE AND DUMPING MEMORY (FAQ #4)

PUBLISHED INFORMATION (LICENSE EXCEPTION TSU; FAQ #4)

SOFTWARE THAT PERMITS AUTOMATIC UPDATES AND ANTI-VIRUS TOOLS (FAQ #8)

SOFTWARE THAT ONLY LEAVES EVIDENCE OF A SUCCESSFUL SECURITY BREACH WITHOUT FURTHER COMPROMISING OR CONTROLL[ING] THE SYSTEM (FAQ #11)

SOFTWARE THAT IS DESIGNED TO DESTROY DATA OR SYSTEMS (FAQ #11)

PORT SCANNERS, PACKET SNIFFERS, AND PROTOCOL ANALYZERS (FAQ #12)

VULNERABILITY SCANNER WHICH JUST FINDS VULNERABILITIES IN A SYSTEM WITHOUT ACTUALLY EXPLOITING THEM AND EXTRACTING DATA (FAQ #12)

ZERO DAY EXPLOITS (FAQ #15)

OPEN SOURCE SECURITY TOOLS (E.G., METASPOLIT, KALI LINUX) (FAQ #21)

GENERAL PURPOSE TOOLS, SUCH AS IDES (FAQ #29)

ETRAC QUESTION #1

ITEMS EXPRESSLY COVERED:

- INFORMATION "REQUIRED FOR" DEVELOPING, TESTING, REFINING, AND EVALUATING "INTRUSION SOFTWARE", IN ORDER, FOR EXAMPLE, [] TO CREATE A CONTROLLABLE EXPLOIT THAT CAN RELIABLY AND PREDICTABLY DEFEAT PROTECTIVE COUNTERMEASURES AND EXTRACT INFORMATION (FAQ #4)
- INFORMATION ON HOW TO PREPARE THE EXPLOIT FOR DELIVERY OR INTEGRATE IT INTO A COMMAND AND DELIVERY PLATFORM (FAQ #4)
- THE DEVELOPMENT OR PRODUCTION OF THE COMMAND AND DELIVERY PLATFORM ITSELF (FAQ #4)
- TECHNICAL DATA SENT TO AN ANTI-VIRUS COMPANY OR SOFTWARE MANUFACTURER IF THE DATA WILL NOT BE MADE PUBLICLY AVAILABLE (FAQ #10)
- INFORMATION FOR THE DEVELOPMENT OF "INTRUSION SOFTWARE" THAT MAY ACCOMPANY THE DISCLOSURE OF AN EXPLOIT (FAQ #24)
- JAILBREAKING TECHNOLOGY FOR SOFTWARE THAT MEETS THE DEFINITION OF 4D004 (FAQ #26)
- EVERYTHING ELSE "REQUIRED" FOR THE "DEVELOPMENT" OF INTRUSION SOFTWARE
  - "REQUIRED" IS MET SO LONG AS THE INFORMATION IS DIRECTED TO THE "INTRUSION " ASPECTS OF THE SOFTWARE AND NOT JUST GENERIC INFORMATION THAT IS NOT RESPONSIBLE FOR THE CONTROLLED ITEM. 15 C.F.R. § 772.
  - "DEVELOPMENT" IS MET SO LONG AS THE INFORMATION IS RELATED TO DESIGN, DESIGN RESEARCH, DESIGN ANALYSES, DESIGN CONCEPTS, ETC. 15 C.F.R. § 772.

ETRAC QUESTION #1

LEGITIMATE EXAMPLE OF WHAT IS PROHIBITED:

- PROPRIETARY TRAINING COURSE MATERIALS PROVIDED OUTSIDE OF THE U.S. OR TO NON-U.S. PERSONS (I.E., INFORMATION ON HOW TO PREPARE AN EXPLOIT FOR DELIVERY OR INTEGRATE IT INTO A COMMAND AND DELIVERY PLATFORM) (FAQ #4)

ETRAC QUESTION #1

- PRESUMPTION OF DENIAL FOR EXPORTS
- “THERE IS A POLICY OF PRESUMPTIVE DENIAL FOR ITEMS THAT HAVE OR SUPPORT ROOTKIT OR ZERO-DAY EXPLOIT CAPABILITIES”
- MANY LEGITIMATE USES FOR ROOTKIT AND ZERO-DAY EXPLOIT CAPABILITIES

ETRAC QUESTION #1

LEGITIMATE EXAMPLE OF WHAT IS PROHIBITED:

- DELIVERY OF A SECURITY REPORT TO NON-U.S. COMPANIES, U.S. SUBSIDIARIES LOCATED ABROAD, OR NON-U.S. PERSONS AT A U.S. COMPANY

OFFENSIVE® security
WWW.OFFENSIVE-SECURITY.COM

PENETRATION TEST REPORT

MegaCorp One
August 10th, 2013

ETRAC QUESTION #1

LEGITIMATE EXAMPLE OF WHAT IS PROHIBITED:

- PROVISION OF SECURITY CONSULTING SERVICES OUTSIDE OF THE U.S. AND TO NON-U.S. COMPANIES (ASSUMING THAT PERFORMANCE OF THE SERVICES REQUIRES THE EXPORT OF 4D004 SOFTWARE "MODIFIED FOR THE GENERATION, OPERATION OR DELIVERY OF, OR COMMUNICATION WITH 'INTRUSION SOFTWARE'")

ETRAC QUESTION #1

LEGITIMATE EXAMPLE OF WHAT IS PROHIBITED:

- SECURITY RESEARCHER'S COMMUNICATIONS BEYOND AN EXPLOIT WITH NON-U.S. COMPANIES, U.S. SUBSIDIARIES LOCATED ABROAD, OR NON-U.S. PERSONS AT A U.S. COMPANY

ETRAC QUESTION #2

"IS IT POSSIBLE TO DEVELOP A LICENSE EXCEPTION, INCLUDING BUT NOT LIMITED TO DEEMED EXPORTS AND INTRA-CORPORATE TRANSFERS, THAT WILL ALLOW LEGITIMATE CYBERSECURITY RESEARCH TO PROCEED WITHOUT LICENSING DELAYS AND COMPLIANCE BURDEN? IF SO, WHAT ARE THE PROVISIONS OF SUCH A LICENSE EXCEPTION?"

ETRAC QUESTION #2

BEST APPROACH:

- REMOVE TECHNOLOGY CONTROLS ALTOGETHER
- THE PROPOSED RULE DOES NOT CONTROL EXPLOITS BECAUSE WE RECOGNIZE THEY ARE NECESSARY FOR RESEARCH AND LEGITIMATE END USE
- WHY THEN WOULD WE CONTROL THE INFORMATION REQUIRED TO DEVELOP AN EXPLOIT WHEN WE DO NOT EVEN CONTROL THE EXPLOIT ITSELF? THIS MAKES NO SENSE.
  - THIS WOULD BE LIKE CONTROLLING THE INSTRUCTIONS ON HOW TO DEVELOP A MISSILE, BUT NOT CONTROLLING THE MISSILE ITSELF.

ETRAC QUESTION #2

ALTERNATIVE APPROACHES (ALL WOULD BE NEEDED, NOT JUST SOME):

- LICENSE EXCEPTION FOR EDUCATION AND TRAINING
- LICENSE EXCEPTION FOR INTRA-COMPANY TRANSFERS
- LICENSE EXCEPTION FOR EXPORTS TO U.S. SUBSIDIARIES
- LICENSE EXCEPTION FOR EXPORTS TO CERTAIN FRIENDLY COUNTRIES
- LICENSE EXCEPTION FOR TECHNOLOGY EXCHANGES RELATED TO SECURITY RESEARCH AND DEVELOPMENT

ETRAC QUESTION #2

EDUCATION AND TRAINING EXCEPTION

- EXPORTS OR REEXPORTS OF EDUCATIONAL AND TRAINING TECHNOLOGY AND RELATED ITEMS PROVIDED AS PART OF A COURSE OR OFFERING MADE GENERALLY AVAILABLE TO THE PUBLIC

ETRAC QUESTION #2

INTRA-COMPANY TRANSFERS

- EXPORTS OR REEXPORTS OF TECHNOLOGY AND RELATED ITEMS BY A U.S. COMPANY AND ITS SUBSIDIARIES TO FOREIGN NATIONALS WHO ARE EMPLOYEES, CONTRACTORS, OR INTERNS OF A FOREIGN COMPANY THAT IS A PARENT, SUBSIDIARY, OR AFFILIATE OF THE U.S. COMPANY

ETRAC QUESTION #2

EXPORTS TO U.S. SUBSIDIARIES

- EXPORTS OR REEXPORTS OF TECHNOLOGY AND RELATED ITEMS TO ANY U.S. SUBSIDIARY, WHEREVER LOCATED, PROVIDED THAT SUCH ITEM IS FOR INTERNAL COMPANY “USE” OF THE ITEM

ETRAC QUESTION #2

EXPORTS TO CERTAIN FRIENDLY COUNTRIES

- EXPORTS OR REEXPORTS OF TECHNOLOGY AND RELATED ITEMS TO ‘PRIVATE SECTOR END-USERS’ THAT ARE LOCATED IN A COUNTRY LISTED IN SUPPLEMENT NO. 3 FOR INTERNAL COMPANY “USE” OF THE ITEM

ETRAC QUESTION #2

TECHNOLOGY EXCHANGES RELATED TO SECURITY RESEARCH AND DEVELOPMENT

- EXPORTS OR REEXPORTS OF TECHNOLOGY AND RELATED ITEMS WITHIN AND ACROSS COMPUTER SECURITY RESEARCH AND DEVELOPMENT TEAMS FOR DISCOVERING, EVALUATING, AND COUNTERING THREATS, VULNERABILITIES, AND EXPLOITS TO COMPUTER OR NETWORKS, PROVIDED THAT SUCH THREATS, VULNERABILITIES, OR EXPLOITS ARE MADE KNOWN OR WILL BE MADE KNOWN TO THE SOFTWARE VENDOR OR PUBLISHER
  - COVERS BUG BOUNTY PROGRAMS
  - COVERS CAPTURE THE FLAG PROGRAMS

ETRAC QUESTION #3

"IS THERE A LICENSE REQUIREMENT (COMBINATION OF DESTINATION/END USER/END USE) AND REGULATORY INTERPRETATION THAT WOULD ADDRESS THE EXCHANGES OF TECHNOLOGY THAT ARE OF CONCERN (I.E., THOSE NOT INTENDED TO ULTIMATELY IMPROVE CYBERSECURITY) THAT WOULD RESULT IN NO LICENSING BURDEN ON LEGITIMATE TECHNOLOGY EXCHANGES?"

ETRAC QUESTION #3

KEY CONCEPTS:

- BROAD EDUCATIONAL AND TRAINING EXCEPTION
- BROAD EXCEPTION FOR R&D WHERE VULNERABILITY WILL BE MADE KNOWN TO THE VENDOR
- BROAD EXCEPTION FOR EXPORTS TO FRIENDLY COUNTRIES AND U.S. SUBSIDIARIES WHERE SUCH ITEMS ARE FOR INTERNAL COMPANY USE

ETRAC QUESTION #4

"IF NONE OF THE MEASURES ABOVE WOULD BE ADEQUATE, WHAT CHANGES TO THE CONTROL TEXT, INCLUDING THE DEFINITION OF "INTRUSION SOFTWARE," WOULD BE REQUIRED TO ENSURE THAT LEGITIMATE CYBERSECURITY RESEARCH WILL NOT BE AFFECTED?"

ETRAC QUESTION #4

- FOCUS ON INTRUSION IS MISGUIDED; ITS WHAT HAPPENS AFTER THE INTRUSION OCCURS THAT MATTERS
- SURVEILLANCE SOFTWARE IS OFTEN THE PAYLOAD OF THE MALICIOUS INTRUSION; THESE PAYLOADS CAN BE DELIVERED MANY OTHER WAYS

QUESTIONS?