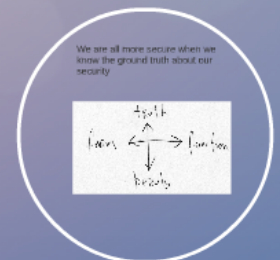
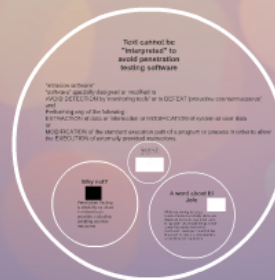
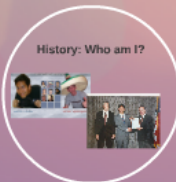
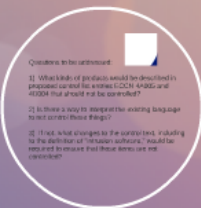
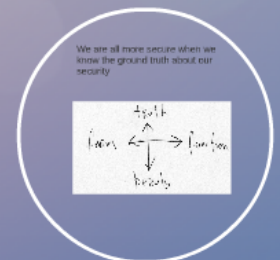
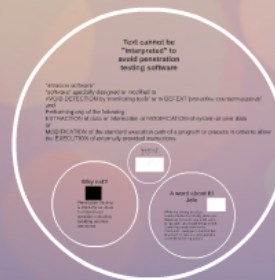
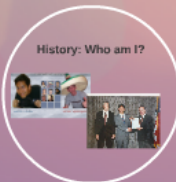
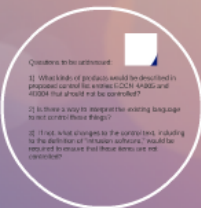


Penetration Testing Software: An Annoying Amount of Detail in 15 Minutes



Dave@immunityinc.com - 786-263-9749 - @daveaitel

Penetration Testing Software: An Annoying Amount of Detail in 15 Minutes



Dave@immunityinc.com - 786-263-9749 - @daveaitel



Questions to be addressed:

- 1) What kinds of products would be described in proposed control list entries ECCN 4A005 and 4D004 that should not be controlled?
- 2) Is there a way to interpret the existing language to not control these things?
- 3) If not, what changes to the control text, including to the definition of "intrusion software," would be required to ensure that those items are not controlled?

History: Who am I?



VERSUS MODE



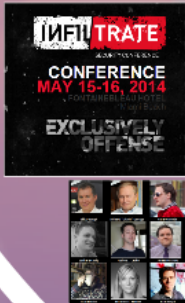
Dave Aitel



Brad Spengler



History: Immunity and Penetration Testing Tools






**Covered by
"Intrusion
Software"**

CANVAS, INNUENDO and SILICA



We are in the unusual situation of regulating as "intrusion software" more things that are almost never used for real intrusions than things that are.

File Listeners Session Help

 Target Host  Stop Exploit  OS Config

Current Callback 192.168.1.16 Current Target(s) 127.0.0.1

 Screen Shots

Modules Search

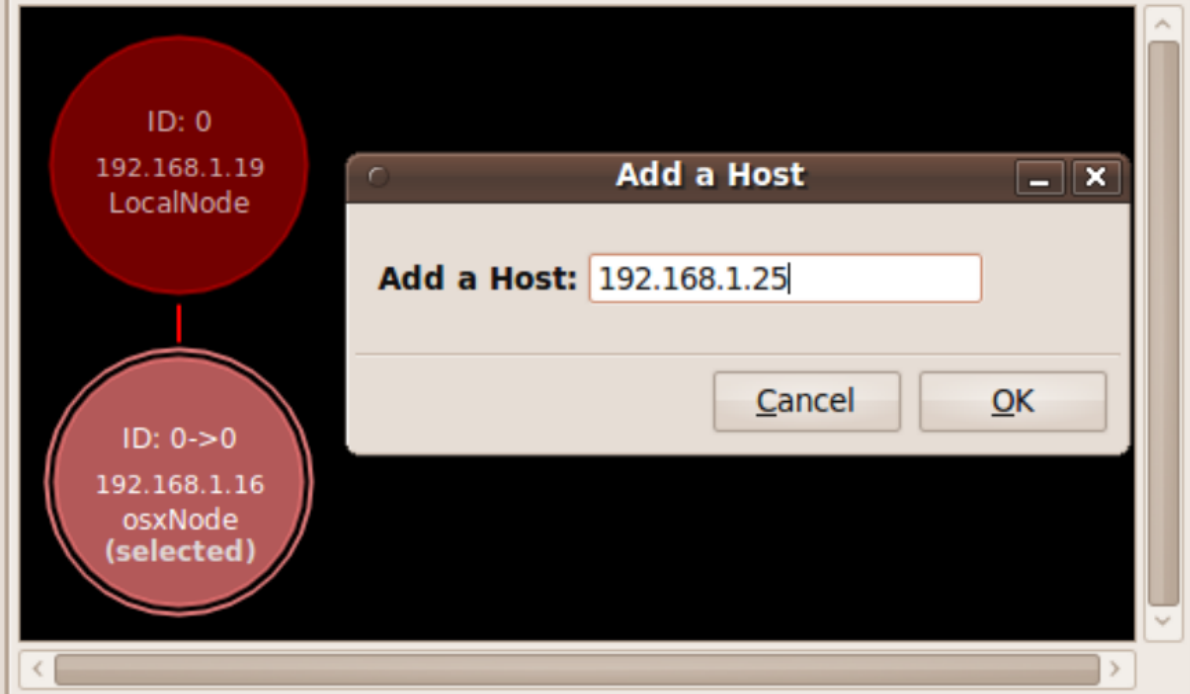
ALL clientd GO

☒ Raw ☐ Regex

Name	Description
acrobat_exec	Acrobat/Foxit Reader
adobe_shockwave_rclschunk	Adobe Shockwave rclschunk
ms10_026	MPEG Layer-3 codec
java_docbase	Java IE Plugin "docbase"
firefox_appendchild	Mozilla Firefox Use-
client_side_report	Creates spreadsheet
clientd	HTTP Server for client
pty_shell	Grabs a shell with a
-- 8 results for that query --	

Node Tree Exploit Description

Node Management CANVAS World Map CmdLine



Current Status Canvas Log Debug Log Data View

Status	Action	Start Time	End Time	Information
▶ 000000	ClientD started on 192.168.1.19:8080...	02:17:41 PM	02:18:09 PM	ClientD

Set Covertness: 1.0

ApplicationsPlaces

SILICA 7.22beta1

- Uptime: 0:01:23 | APs: 34 | Ad-Hoc: 0 | Clients: 8 | Probes: 12 | Most Active Probes: 'Marisa: 1 STEFY: 1 falabella'

SessionFilter

SILICA

START

STOP

PREFERENCES

UPDATE

IMMUNITY

Network Listing

Cookie Viewer

Fake AP

Passwords

Log

Info

Key Recovery

	▼	Clients	ESSID	Data	Quality	Signal	Channel	Encryption	Cipher	Type	Auth
IC:68:42		0:0	Speedy-6842A2	0	95%	-74dBm	11	WPA	TKIP, AES/CCMP	AP	PSK, WPS(ON)
59:D3:A1		0:1	mengueche	0	32%	-74dBm	6	WPA	AES/CCMP, TKIP	AP	PSK, WPS(ON)
F7:D4:A1		0:0	ESTUDIO	0	31%	-75dBm	6	WPA	AES/CCMP, TKIP	AP	PSK, WPS(ON)
DD:54:40		3:0	La Estacion Casa de Arte	0	30%	-76dBm	1	WPA	AES/CCMP, TKIP	AP	PSK, WPS(ON)
FE:8A:D1		0:0	SPEEDYWIFI	0	27%	-78dBm	11	WEP		AP	
F0:9E:15		0:0	Speedy_sxwsc4	0	27%	-78dBm	11	WEP		AP	
F7:DB:71		0:0	Home	0	26%	-79dBm					
26:2E:4C		0:0	casita	0	32%	-74dBm					
4C:7E:0C		0:0	Viejo	0	31%	-75dBm					
02:7A:CE		0:0	Trapacero	0	30%	-76dBm	5	WPA	AES/CCMP	AP	PSK, WPS(ON)
DD:61:81		0:0	Fibertel WiFi750	0	27%	-78dBm	11	WPA	AES/CCMP, TKIP	AP	PSK, WPS(ON)
4B:2B:C1		0:0	Viejo	0	27%	-78dBm	11	WEP		AP	WPS(ON)
33:8B:E3		0:0	CINTSAN	0	27%	-78dBm	8	WPA	AES/CCMP	AP	PSK, WPS(ON)
7A:A3:E1		0:0	Lidia	0	26%	-79dBm	6	WEP		AP	
11:B0:F4		0:0	THORNFIELD	0	26%	-79dBm	4	WPA	AES/CCMP, TKIP	AP	PSK, WPS(ON)
DD:65:D1		1:0	Fibertel WiFi876	0	25%	-80dBm	11	WPA	AES/CCMP, TKIP	AP	PSK, WPS(ON)
A5:1F:D1		0:0	Fibertel_Prov	0	20%	-84dBm	11	None		AP	
EC:10:CE		0:0	cucc	0	41%	-67dBm	11	WPA	TKIP	AP	PSK
54:51:71		0:0	Fibertel WiFi448	0	40%	-68dBm	1	WPA	AES/CCMP, TKIP	AP	PSK
F1:A1:C1		0:0	Fibertel WiFi	0	36%	-71dBm	1	WPA	TKIP	AP	PSK
DD:61:83		0:0	wifi gasparovic	0	36%	-71dBm	1	WPA	AES/CCMP, TKIP	AP	PSK
56:9E:54		0:0	Telefonos 5484	0	36%	-71dBm	1	WPA	AES/CCMP, TKIP	AP	PSK, WPS(LOCKED)

Discover key

Edit Key

Edit SSID

Sniff on this channel

Disable this network

WPS

Get WPS PIN (full bruteforce)

Get WPS PIN (try only default pins)

Get WPS Info

Storing recovered key in database: 90:67:1C:68:42:A8 []

Recover Key

Clear window

Expand

Channel Hop

silicau@ubuntu: ~

Terminal

tail

SILICA 7.22be...

Displays

Pictures



INNUENDO – An Advanced Penetration Testing tool for modeling Advanced Attackers

Overview

INNUENDO raises the bar for the state of the art in persistence and data exfiltration solutions. Based on a flexible, modular architecture, INNUENDO offers nation-grade advanced attack capabilities to commercial penetration testing teams.



[Download Innuendo slick PDF](#)

- **INNUENDO** breaks from the current penetration testing model by using a message passing protocol that is completely decoupled from any transport layer. This allows for a wide range of communication channels which are easily integrated into your INNUENDO solution. Examples include: HTTPS, DNS, ICMP, PDF, Social Media, and steganographic injection into popular image hosting services.
- Persistence can be maintained via any one of many ways, determined at deploy time. That means no static indications of compromise! Persistence methods are modular and updatable throughout the life of the deployment. **INNUENDO** functionality can be written, deployed and updated in Python without ever touching disk and is encrypted and signed for a specific **INNUENDO** instance on deployment.
- Each deployed **INNUENDO** has a unique SHA1 hash which prevents one-stop binary fingerprinting.
INNUENDO can be deployed entirely from memory via e.g. a CANVAS exploit, a post-exploitation CANVAS module, or from another INNUENDO instance. INNUENDO can run as an injected DLL or as its own process.

INNUENDO instances employ strong encryption for C&C messages, which renders the communications opaque to listeners and frustrates post-event forensics.



Browse Events

Search Results :
226

Date	Parent Binary	Binary	Cmdline	Username	Station	
April 10, 2014, 3:26 p.m.	C:\Windows\system32\svchost.exe	C:\Windows\System32\slui.exe	C:\Windows\System32\	WIN-MEP0P1QJB13\	WIN-MEP0P1QJB13	
April 10, 2014, 3:03 p.m.	C:\Windows\system32\services.exe	C:\Windows\system32\taskhost.exe	taskhost.exe \$(Arg0)	NT AUTHORITY\LOCAL SERVICE	WIN-MEP0P1QJB13	
April 10, 2014, 2:56 p.m.	C:\Windows\system32\svchost.exe	C:\Windows\System32\slui.exe	C:\Windows\System32\	WIN-MEP0P1QJB13\	WIN-MEP0P1QJB13	
April 10, 2014, 2:55 p.m.	C:\Program Files\Citrix\SelfServicePlugin\SelfServicePlugin.exe	C:\Program Files\Citrix\SelfServicePlugin\SelfService.exe	"C:\Program Files\Ci	WIN-MEP0P1QJB13\	WIN-MEP0P1QJB13	
April 10, 2014, 2:48 p.m.	C:\Program Files\Google\Update\GoogleUpdate.exe	C:\Program Files\Google\Update\GoogleUpdate.exe	"C:\Program Files\Go	NT AUTHORITY\SYSTEM	WIN-MEP0P1QJB13	
April 10, 2014, 2:48 p.m.	C:\Windows\system32\SearchIndexer.exe	C:\Windows\system32\SearchFilterHost.exe	"C:\Windows\system32	NT AUTHORITY\SYSTEM	WIN-MEP0P1QJB13	

INFILTRATE

SECURITY CONFERENCE

CONFERENCE
MAY 15-16, 2014

FONTAINEBLEAU HOTEL

Miami Beach

**EXCLUSIVELY
OFFENSE**



Bill Arbaugh



Richard "Dickie" George



Cesar Cerrudo



Zachary Cutlip



Joshua J. Drake



James Forshaw



Sean Heelan



Suzanne E. Kecmer



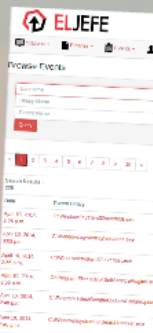
Paul Royal

Covered by "Intrusion Software"

CANVAS, INNUENDO and SILICA



We are in the unusual situation of regulating as "intrusion software" more things that are almost never used for real intrusions than things that are.



Text cannot be "interpreted" to avoid penetration testing software

"intrusion software"

"software" specially designed or modified to

AVOID DETECTION by 'monitoring tools' or to DEFEAT 'protective countermeasures' and

Performing any of the following :

EXTRACTION of data or information or MODIFICATION of system or user data

or

MODIFICATION of the standard execution path of a program or process in order to allow the EXECUTION of externally provided instructions.

The Unspoken Casualty:
Custom tools, which are
often used for commercial
consulting



Why not?



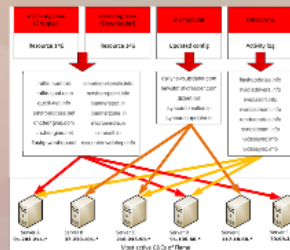
Penetration Testing
is explicitly as close
to malware as
possible, including
avoiding counter-
measures

A word about EI Jefe



While not aiming to defeat
countermeasures initially, when you
detect an intrusion, you often want
to "go dark" and install things which
cannot be easily detected or
monitored - next-gen CrowdStrike/
Mandiant/EI Jefe are all potentially
covered by the regulation!

Why not?



Penetration Testing
is explicitly as close
to malware as
possible, including
avoiding counter-
measures

A word about El Jefe



While not aiming to defeat countermeasures initially, when you detect an intrusion, you often want to "go dark" and install things which cannot be easily detected or monitored - next-gen CrowdStrike/ Mandiant/El Jefe are all potentially covered by the regulation!

The Unspoken Casualty: custom tools, which are often used for commercial consulting

SERVICES OVERVIEW

Consulting Services

- Adversary Simulation
- Application Vulnerability Analysis
- Digital Executive Protection
- Exploit Development & Reverse Engineering
- Network Security Assessment
- Penetration Testing
- Process Review
- Source Code Analysis
- Web Application Testing
- Wireless Security Assessment
- Consultants
- When Choosing a Service Provider

Consulting Services Overview

Immunity offers specialized attack and assessment services, including penetration testing, application assessments, vulnerability analysis, reverse engineering, architecture review and source code review.

New clients are often surprised to learn about the existence of unpublicized or unpatched vulnerabilities in exposed systems. Repeat clients benefit from familiarity and a client-specific knowledge-base as Immunity and the client work together over time.

All clients learn about real levels of exposure - not misleading false negative or false positive reports as generated by typical commercial vulnerability scanners.

Immunity's team always employs the perspective and philosophy of an attacker. This provides the client with a realistic picture of their level of exposure and an ability to adequately measure the risk associated with technology deployments.

The links here provide an overview of Immunity's methodology and approach to delivering assessment services. For more information, please contact sales@immunityincdotcom.



SERVICES OVERVIEW

Consulting Services

Adversary Simulation
Application Vulnerability Analysis
Digital Executive Protection
Exploit Development & Reverse Engineering
Network Security Assessment
Penetration Testing
Process Review
Source Code Analysis
Web Application Testing
Wireless Security Assessment
Consultants
When Choosing a Service Provider

Consulting Services Overview

Immunity offers specialized attack and assessment services, including penetration testing, application assessments, vulnerability analysis, reverse engineering, architecture review and source code review.

New clients are often surprised to learn about the existence of unpublicized or unpatched vulnerabilities in exposed systems. Repeat clients benefit from familiarity and a client-specific knowledge-base as Immunity and the client work together over time.

All clients learn about real levels of exposure - not misleading false negative or false positive reports as generated by typical commercial vulnerability scanners.

Immunity's team always employs the perspective and philosophy of an attacker. This provides the client with a realistic picture of their level of exposure and an ability to adequately measure the risk associated with technology deployments.

The links here provide an overview of Immunity's methodology and approach to delivering assessment services. For more information, please contact sales@immunityincdotcom.



"Unauthorized"

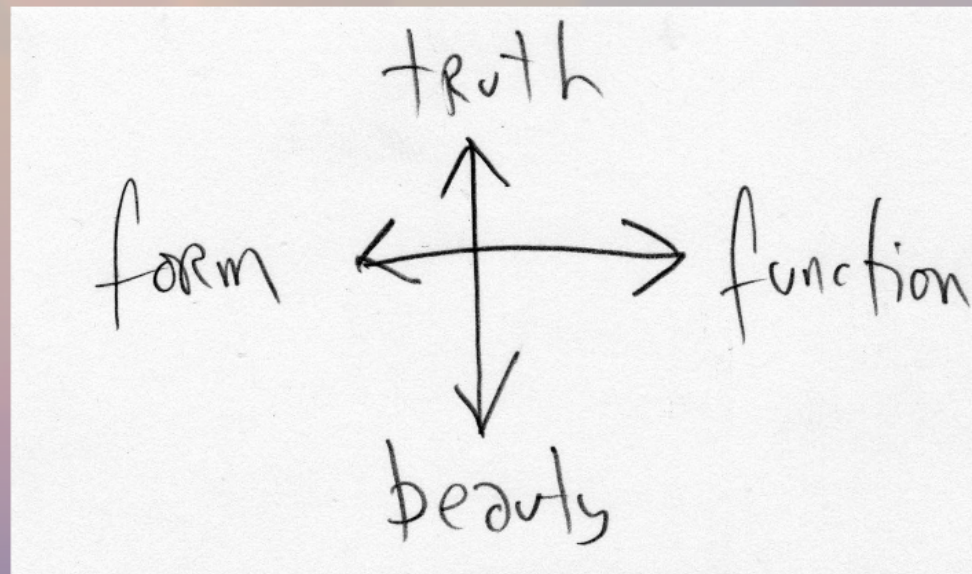
3) If not, what changes to the control text, including to the definition of "intrusion software," would be required to ensure that those items are not controlled?

4.E.1.c.

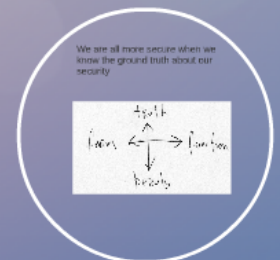
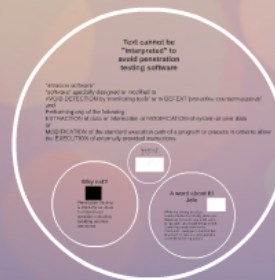
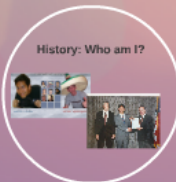
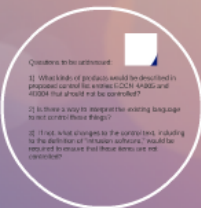
"Technology" for the development of "intrusion software".

Potentially covered a lot of research software needed to understand risk.

We are all more secure when we know the ground truth about our security



Penetration Testing Software: An Annoying Amount of Detail in 15 Minutes



Dave@immunityinc.com - 786-263-9749 - @daveaitel