

009 - 46F-EB9 - Evading Client Honeypots - Jason Ortiz - SAET

CERLAS

the center for education and research in information assurance and security

Evading Client Honeypots

Jason Ortiz, Ankur Chakraborty, Pascal Meunier

Client-side Attacks

Client makes a request to a malicious or compromised server
 Server acts to infect the client, targeting some of many vulnerabilities in applications
 Increasing number of exploits due to better serverside security
 Large number of opportunities (apps, plug-ins...) are vulnerable to exploits or attacks



Client Honeypots

Client honeypots have detected and analyzed thousands of attacks

Easily detect drive-by downloads and browser



or application exploits
➤ Check of system changes (registry changes, process creation/termination)
➤ Actively seek to be attacked opposed to traditional honeypots

Targeting Real Users by Hiding Malicious Intent

We observed that malicious websites employ social engineering to convince users of legitimate interaction.

Methodology

We surveyed approximately 5000 websites using Honeyclient and manual navigation

Observation We found 43 attacks, many of them using a form of social engineering to gain user's trust

• Example Rogue Applications



Application appears as an *antivirus* software It is actually malware (usually spyware)

Evading Honeypots by Hiding Malicious Content

We hypothesize that malicious websites could employ several techniques designed to evade client honeypots.

Detect presence of VM (active) Detect automated clicks (active) Detection using time restraints (active) Use forms and CAPTCHA (passive) ≻But how difficult is it?







A forged thread report informs the user their computer is infected with malware
 User is tricked into running a 'scan' of their system to find the infections

'Scan' finds hundreds of problems
 Application informs the user they must register and purchase the full version of the software to remove the threats
 User effectively pays for malware and disclosure of personal info

🧔 Applications Places Syst	tem 📅 🕲 👷 🙀 🛛 🗗 🗖 🖻 Jason Ortiz	z 👅 🛛 🎄 🍷 🚍 🔄 🍬 Thu Feb 1 <u>2, 10:05</u> AM
a2e706995f163b5b91c8197458 - VMware Server Console – •		
Eile Edit <u>V</u> iew H <u>o</u> st VM Tabs Help		
Power Off Suspend Power	On Reset Snapshot Revert Full Screen Quick Switch	[양] Summary Console
Inventory 🛛 🕺 💣 batmobile 🗙 🏟 Firewall VM [v3] 🗙 👘 a2e706995f163b5b91c8197458 🗙		
🚯 Firewall VM [v3	D Delice® Antivirum Mazilla Firefox	
🔂 cab082873a8	Edit View History Bookmarks Tools Help	
🔂 d32c27db1f5e		
🛱 d105e36addb	Image: Im	
🖞 0f65796784e0 👔 Most Visited 🐢 Getting Started 🔊 Latest Headlines 🗋 Customize Links 🗋 Free Hotmail 🗋 Windows Media 🗋 Windows		
🖆 226af0c181fa		<u> </u>
a2e706995†16	XP Police® Antivirus 1 Year License Subscription includes new version undates, definition undates, standart	Baumant Tunati
14b18d8c11c	customer support for 1 Year. When the license will be expired - you will	
658c035c87b 6 6 6 6 6 6 6 6 6 6 7 7 6 7	informed via e-mail or phone by our customer support. For only \$39,99 .	Card Number*:
dd0f4fd6676fa		Expiration Date*: 🛛 🚽 🚽 👘
estcle79aa29		CVV2*: What is CVv
C 20091611000	XP Police® Antivirus LIFETIME UNLIMITED License	Namatu
a353e2398ec	Subscription includes new version updates, definition updates, standart customer support for 6 Months. When the license will be expired - you will	
2826622832e	informed via e-mail or phone by our customer support.	
Af7002d701f2	Only Coday infined other for only 239.22 39.99 GSD.	Email*:
		Country*: Afghanistan
t f5a5c982c6ae	XP Police® Antivirus Platinum Support	Agnanistan
3bffa7ach24c1	Includes personal manager, e-mail, tickets support 24/7. With our platinum	State*: Alabama
2 7e23563784d	support you will resolve all problems with your operation system during 24 hours! Add this option to your order now for special price!	Address*:
82bd2c9d7a91	For only \$19.99 .	City*:
44d7870867d		Zin*:
h 6c2cc7f6da74		
		Phone*:
A You chould upgrade your virtual machine		
🖸 💿 [SourceForge.net: 📧 [jdortiz@batmobil 🗱 a2e706995f163b5 😨 jdortiz@batmobile 🔚 Honeyclient Data 🔀		

Created a page designed to detect automation (clicking)
 Created a script which launched only after 15 seconds
 Logged information on server log page



Future Plans: Preventing Evasion

Bare-Metal Implementation of client honeypots

Traditional honeypots use virtual environments to contain attacks experienced

Malicious entities can detect presence of virtual environment (See proof of concept above) Implementing a model of user interaction Vary amount of time spend on a single page (time attacks not prevented but harder) Parse for hidden links and avoid clicking them Be able to fill out forms and defeat CAPTCHA

Requires computer we can reimage
 Requires remote logging of events
 Data might get corrupted from attack
 Attack might destroy its own trail





MITRE Data Set, Kathy Wang

Detecting the Presence of Virtual Machines Using the Local Data Table, Danny Quist, Val Smith

Ask for others and more details!

PURDUE UNIVERSITY



