SOCIAL ENGINEERING AND ROGUE SOFTWARE

IT SECURITY ACADEMY

INTRODUCTION





F

SOCIAL ENGINEERING EFFORTS AIM

to furtively goad people into doing what another person wants them to do Social engineering attacks bypass most security solutions

WE USUALLY FALL VICTIM TO MANIPULATION WHEN:

- We're doing everyday tasks in an environment we know well
- They pertain to non-typical operations: when something requires time and effort, we usually choose the simplest, most obvious solution
- F

We rely on computer systems and software too much



INTRODUCTION

THE SUCCESS OF SOCIAL engineering largely depends on attackers having obtained a large amount of data related to the victim. As people's views on privacy have undergone a radical change recently, obtaining personal information may be very easy

AT WWW.SOCIAL-ENGINEER.ORG you'll find both manuals and social engineering tools



manipulation tactics





GREED (EVERY MAN HAS HIS PRICE...)

Personnel with low-paying jobs are especially susceptible to social engineering; they're people who believe they are paid less than they should be or who feel unaccepted in the workplace



The attacker ensures the victim that the responsibility for taking or not taking a decision or action is someone else's (a co-worker's or your boss's)



T SECURITY ACADEMY www.SecAcademy.com

manipulation tactics



READINESS TO HELP (COULD YOU GIVE ME A HAND, PLEASE?)

The attacker is a newly hired, perplexed worker, or an attractive blonde who repeatedly forgets passwords, or an elderly person who isn't technology-savvy. Adapting these roles, the attacker finds it easy to obtain confidential data or gain access to a system



RELATIONSHIP OF TRUST (I'VE HELPED YOU, WHY CAN'T YOU DO ME A FAVOUR?)

In this scenario, the attacker helps another person solve a problem he had triggered earlier (such as re-connecting to the Internet or retrieving a service) and expects reciprocation from the victim



IT SECURITY ACADEMY www.SecAcademy.com

manipulation tactics



EMOTIONAL BLACKMAIL (YOU HAVE TO HELP ME!)

Most of us can't leave a person in need and will help out the attacker: even if it's just because we want them to stop bothering us



FRIENDSHIP (YOU'RE THE ONLY ONE WHO UNDERSTANDS ME...) First the attacker fosters a friendly

relationship with the victim and then exploits this trust





manipulation tactics



FEELING GUILTY (SO YOU WON'T DO EVEN THIS FOR ME...)

When the attacker is able to make the victim feel guilty, this will make it easier to convince the victim to do as requested



READINESS TO CO-OPERATE (LET'S DO THIS TOGETHER!)

The attacker suggests that the easiest way out of a problem (which was often caused by the attacker) is to work on it as a team



IT SECURITY ACADEMY www.SecAcademy.com

manipulation tactics



FEAR (DO THIS, OR ELSE...) Blackmailing or making the victim fear the consequences may often make him co-operate with the attacker

0.





T SECURITY ACADEMY www.SecAcademy.com



engineering attacks



SPOOFING IDENTITIES USING A SERVICE:



\$

http://fakenamegenerator.com

http://spooftel.com/

http://fakemytext.com/

SOCIAL ENGINEER TOOLKIT ATTACKS:



www.social-engineer.org



Metasploit



IT SECURITY ACADEMY www.SecAcademy.com

ROGUE SOFTWARE



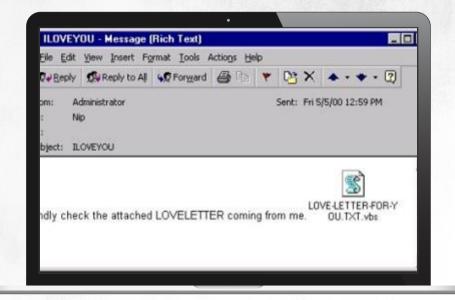
AN EXCEEDINGLY POPULAR

and effective social engineering attack (usually launched in large-scale campaigns that target random Internet users). FraudTools, or rogue software is the software users are tricked into launching, installing or even purchasing



THIS TYPE OF ATTACK IS EASY

to automate. A case in point was a 2000 attack created by a hacker called Spyder, who mass-mailed email massages with a VBScript attached (VBScript LOVE-LETTER-FOR-YOU.TXT.vbs)







ROGUE SOFTWARE



OVER THREE MILLION PEOPLE wanted to find out who's in love with them and why and opened the attachment despite not knowing the source of the email



MASS-MAILING ROGUE EMAILS

that tell recipients they have won money, received a great work proposal or request them to be their friends in a social networking site are still among the most common ways to obtain confidential information about targets





FAKE EMAILS

To file in for the processing of your prize winnings, you are advised to contact our Certified and Accredited claims agent for category "A" winners with the information below:

Name: Mr.Henk Wolter Email: agntoffice07@aim.com Phone: 0031 633 690 563 Fax: : 0031 847 553 129 Amsterdam . The Netherlands

...

You are adviced to provide him with the following necessary information for vetting process which is a standard practice just to ensure that we are dealing with the right individual.

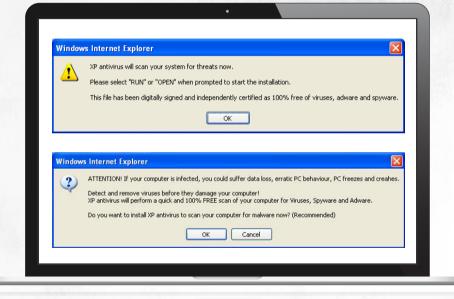


FRAUDTOOLS: XP ANTIVIRUS The First Warning

SOCIAL ENGINEERING ATTACKS employing rogue antiviruses are extremely effective, as proved by the thousands of people who bought fake antivirus scanners in 2008

THE FIRST STEP OF THE ATTACK

was displaying an alarming-sounding warning message that looked like Windows messages





 \bigcirc

FRAUDTOOLS: XP ANTIVIRUS The First Warning



THE WARNING WAS WRITTEN IN GOOD ENGLISH and contained a clear, precise prompt: Detect and remove viruses before they damage your computer!

IF YOU STILL DIDN'T KNOW

what to do, the OK button was highlighted by default



WHEN YOU CLICKED OK, YOU WERE TOLD that scanning and removal will be started in a moment, and that XP Antivirus is digitally signed, secure and independently certified as 100% free of viruses, adware and spyware



www.SecAcademy.com

IT SECURITY ACADEMY

FRAUDTOOLS: XP ANTIVIRUS You've got a problem, but we can solve it

SCANNING WAS STARTED simultaneously. In another window you could traced the progress of the scanning, even though the user did not agree to install any ActiveX controls or to download and start the antivirus

THE SCAN ALWAYS PRODUCED the same result: the computer was apparently infected with many malicious programs

THE ATTACKERS INFORMED users they could remove the malware quickly and in a secure way: they just need to agree to install XP Antivirus

Detected malicious programs can damage your computer and com your privacy. It is strongly recommended to remove them imm Name Type Risk level	tromis			dangerous spy	
		remove them immed	recommended to	your privacy. It is strongly i	Nar
Spyware.IEMonster.b Spyware CRITICAL	1	CRITICAL			3
Zlob.PornAdvertiser.Xplisit Spyware High		High	Spyware	Zlob.PornAdvertiser.Xplisit	
🕈 Trojan.InfoStealer.Banker.s Trojan Medium		Medium	Trojan	Trojan.InfoStealer.Banker.s	
	0				-



 \mathbf{O}

You can trust us



SO AS NOT TO RAISE

any suspicions, the installer started at that point contained an icon resembling the one used by Windows Security Center and also had a Windows-compliant logo.



THE ATTACKERS ALSO prepared a license agreement users could (but were not forced to) accept before installing

KP antivirus 2008 Installer



This program will download and install XP Antivirus on your PC. By clicking Continue button you accepting our terms and conditions.

Continue



00

You can trust us





 \mathbf{O}

And here's our license agreement

ANTIVIRUS XP 2008 LICENSE AGREEMENT

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING ANTIVIRUS XP 2008. ANTIVIRUSXP2008.COM AND/OR ITS SUBSIDIARIES ARE WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING ANTIVIRUS XP 2008 (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND ANTIVIRUSXP2008.COM BY CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL; MAKE NO FURTHER USE OF THE SOFTWARE, AND **CONTACT THE CUSTOMER SUPPORT TEAM**.

1. LICENSE

THE SOFTWARE WHICH ACCOMPANIES THIS LICENSE (COLLECTIVELY THE "SOFTWARE") IS THE PROPERTY OF ANTIVIRUSXP2008.COM OR ITS LICENSORS AND IS PROTECTED BY COPYRIGHT LAW. WHILE ANTIVIRUSXP2008.COM CONTINUES TO OWN ANTIVIRUS XP 2008, YOU WILL HAVE CERTAIN RIGHTS TO USE ANTIVIRUS XP 2008 AFTER YOUR ACCEPTANCE OF THIS LICENSE. THIS LICENSE GOVERNS ANY RELEASES, REVISIONS, OR ENHANCEMENTS TO ANTIVIRUS XP 2008 THAT ANTIVIRUSXP2008.COM MAY FURNISH TO YOU. IN CASE YOU KEEP USING OUR PRODUCT WITHIN 7 DAYS FOLLOWING THE EXPIRATION OF THE ONE-YEAR PERIOD OF SUBSCRIPTION, YOU ARE AUTOMATICALLY CHARGED FOR THE PRODUCT COST. BY ACCEPTING THIS LICENSE AGREEMENT YOU GIVE YOUR CONSENT THAT THE DETAILS OF YOUR CREDIT

CARD ARE BEING RETAINED WITHIN THE ENTIRE PERIOD OF SUBSCRIPTION." IT SECURITY ACADEMY



And here's our license agreement

YOUR RIGHTS AND OBLIGATIONS WITH RESPECT TO THE USE OF THIS SOFTWARE ARE AS FOLLOWS: YOU MAY:

A. USE ONE COPY OF ANTIVIRUS XP 2008 ON ONE (1) SINGLE COMPUTER DURING SUBSCRIPTION PERIOD; B. MAKE ONE COPY OF ANTIVIRUS XP 2008 FOR ARCHIVAL PURPOSES, OR COPY THE ANTIVIRUS XP 2008 ONTO THE HARD DISK OF YOUR COMPUTER AND RETAIN THE ORIGINAL FOR ARCHIVAL PURPOSES;

C. USE ANTIVIRUS XP 2008 ON A NETWORK, PROVIDED THAT YOU HAVE A LICENSED COPY OF ANTIVIRUS XP 2008 FOR EACH COMPUTER THAT CAN ACCESS ANTIVIRUS XP 2008 OVER THAT NETWORK; AND

D. AFTER WRITTEN PERMISSION FROM ANTIVIRUSXP2008.COM, TRANSFER ANTIVIRUS XP 2008 ON A PERMANENT BASIS TO ANOTHER PERSON OR ENTITY, PROVIDED THAT YOU RETAIN NO COPIES OF ANTIVIRUS XP 2008 AND THE TRANSFEREE AGREES TO THE TERMS OF THIS LICENSE;

E. BE INFORMED OF ANY CHANGES OR UPDATES REGARDING THE ANTIVIRUS XP 2008 BY E-MAIL OR ANY OTHER CONTACT METHOD AVAILABLE.

YOU MAY NOT: A. COPY THE PRINTED DOCUMENTATION WHICH MAY ACCOMPANY ANTIVIRUS XP 2008; B. SUBLICENSE, RENT OR LEASE ANY PORTION OF ANTIVIRUS XP 2008; **REVERSE ENGINEER**, **DECOMPILE**, **DISASSEMBLE**, MODIFY, TRANSLATE, **MAKE ANY ATTEMPT TO DISCOVER THE SOURCE CODE OF ANTIVIRUS XP 2008**, OR CREATE DERIVATIVE WORKS FROM ANTIVIRUS XP 2008; C. USE A PREVIOUS VERSION OR COPY OF ANTIVIRUS XP 2008 AFTER YOU HAVE RECEIVED A DISK REPLACEMENT SET

OR AN UPGRADED VERSION. UPON UPGRADING THE SOFTWARE, ALL COPIES OF THE PRIOR VERSION MUST BE DESTROYED; IT SECURITY ACADEMY

And here's our license agreement

2. REFUNDS POLICY

B. OUR 24/7 CUSTOMER SUPPORT SERVICE SHOULD BE CONTACTED FOR ANY TROUBLESHOOTING. CUSTOMER SUPPORT SERVICE SHOULD BE INFORMED IN THE EVENT THE CUSTOMER'S SYSTEM CRASHED FOR ANY REASON, IN ORDER FOR THE CUSTOMER TO BE ENTITLED TO CLAIM A REFUND. IF THE SUPPORT TEAM IS NOT CONTACTED, A REFUND WILL NOT BE MADE.

THIS REDUCES ALL PROBLEMS TO TECHNICAL DIFFICULTIES WHICH WILL BE RESEARCHED AND SOLVED. ANTIVIRUSXP2008.COM IS NOT RESPONSIBLE FOR ANY HELP THE CUSTOMER GETS FROM THIRD PARTY TECHNICIANS. ALSO ANY ACTIONS TAKEN BY THE CUSTOMER ARE MADE AT HIS OR HER RISK.

C. SOME OF OUR PRODUCTS MAY BE UNSUITED TO RUN WITH OTHER SOFTWARE. WE HAVE THE RIGHT TO UNINSTALL INCOMPATIBLE PRODUCTS. WE WILL NOTIFY OUR CUSTOMERS BEFORE UNINSTALLING SUCH PRODUCTS. A CUSTOMER CANNOT CLAIM A REFUND IF THE REASON IS A REQUISITION OR REMOVAL OF CONFLICTING SOFTWARE. COEXISTENCE OF SOME PRODUCTS MAY LEAD TO MANY UNSATISFACTORY EFFECTS AS WELL AS TO SLOW THE CUSTOMER'S SYSTEM. THAT IS WHY THE USAGE OF ANTIVIRUS XP 2008 REQUIRES THE UNINSTALLATION OF PRODUCTS WHICH REPRESENT A RISK TO THE SYSTEM. ...

E. WE ARE NOT LIABLE IF THE CUSTOMER'S SYSTEM WAS RESTORED OR REPAIRED AND A REFUND WILL NOT BE MADE IN SUCH A CASE.

IN A FEW CASES, PROTECTION-RELATED ANTIVIRUS XP 2008 CANNOT DEAL WITH OVERLOADED AND DAMAGED SYSTEMS. IN SUCH CASES, THE ANTIVIRUSXP2008.COM IS NOT RESPONSIBLE.

F. ANTIVIRUSXP2008.COM CANNOT BE HELD RESPONSIBLE FOR ACTIONS PERFORMED BY THE CUSTOMER WHEN NOT USING OUR SOFTWARE.





There's technical support in case you're still not sure

THE SCANNER'S website had a professional look and encouraged users to contact the support centre if need be





 $\Diamond \Diamond$

Great you've installed the program, but...

AFTER THE ATTACKERS CONVINCE their victims to install the rogue antivirus and get rid of all legitimate antiviruses, they start tricking money out of them

TO COAX USERS TO ABANDON

basic security practices and hand over their credit card numbers, the rogue antivirus



TP ANTIVIRUS			🔗 Registration	() Help	
System Scan	XP Antivir	rus 2008: Syster	m scan		
-	Туре	Run type	Name	Details 🗖	
💔 Security	Spyware	C://windows/system	Spyware.IEMonster.d	"Steals password	
	Adware	autorun	Zlob.PornAdvertiser.ba	Adware that disp	
🖄 Privacy	Spyware	autorun	Spyware.IMMonitor program that		
	Backdoor	C://windows/system	Win32.Rbot.fm	An IRC controllec	
🥔 Update	Trojan	autorun	Infostealer.Banker.E	Steals sensitive in	
	Dialer	C://windows/system	Dialer.Xpehbam.biz_dialer	A Dialer that load	
1	Spyware	autorun	Spyware.KnownBadSites	Uses the Window	
🛃 Settings	Trojan	autorun	Trojan. Tooso	Trojan. Tooso is a	
	Trojan	C://windows/system	Trojan.MalGrabber.s	Trojan horse that	
	Trojan	C://windows/system	Trojan.Alg.t	Trojan program ti	
	Rogue	C://Program Files/Tr	TrustedAntivirus	A corrupt and mis	
	Rogue	C://Program Files/Se	. SecurePCCleaner Rogue Securit		
	Trojan	C://windows/system	Trojan.BAT.Adduser.t	This Trojan has a 🗸	
	<			>	
	Scan pro	gress		emove	
		sentationFramework.Luna.ni.		emove	

T SECURITY ACADEMY www.SecAcademy.com \mathbf{O}

FRAUDTOOLS: XP ANTIVIRUS ... It's time you paid...

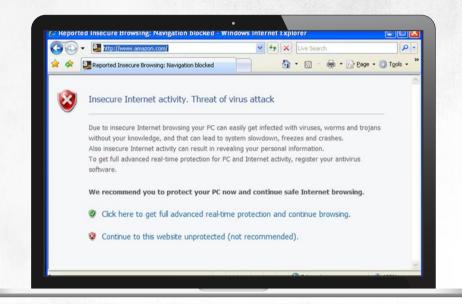


REPLACED A USER'S SCREEN saver with one that simulated the STOP system error message. To conceal this change, it hid the Screen Saver tab from users



INSTALLED AN INTERNET EXPLORER PLUGIN

that intercepted some communications with random websites and displayed a warning that resembled the standard system warning about insecure websites or websites that lack a valid certificate





... or someone will be reading your private messages



REGULARLY (INTRUSIVELY) DISPLAYED reminders about how risky it was to use an infected machine



DISPLAYED A RED SHIELD ALERT on the status bar that warned users about no antivirus being found. It also displayed other warnings at regular intervals







You do trust antiviruses, don't you?

Registered a rogue Security Center window in the system. This Security Center detected XP Antivirus and recommended users to install it

S Windows Security Center	Security Center Help protect your PC	🕏 Windows Security Center	Security Cente
Resources Set the latest security and virus information from Microsoft Check for the latest updates from	Security essentials Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security sesentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel. What's new in Windows to help protect my computer?	Resources Set the latest security and virus Get the latest security and virus Get support for security-related Get support for security-related	Security essentials Security Center helps you to manage your Windows security settings. To protect your computer, make sure the three security essentials are turned ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
Windows Update	🤪 Firewall 🛛 ON 😵	Get help about Security Center Change the way Security Cente	Firewall ON
 Get support for security-related issues 	🍓 Automatic Updates 💿 ON 🛞	Change the way security center	🔱 Automatic Updates 🔹 ON
Get help about Security Center Change the way Security Center	Virus Protection NOT FOUND		Virus Protection • NOT FOUND
alerts me	Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. <u>How does antivirus software help protect my computer?</u> Note: Windows does not detect all antivirus programs. Recommendations		Windows Security Center reports that 'XP antivirus' is inable. Antivirus software helps to protect your computer against viruses and other security threats. Click Recommendations for the suggested actions. Your system might be at a risk now. Note: Windows detect unregistered version of "XP antivirus" Click here to get XP antivirus License
	Manage security settings for:		Manage security settings for:
	🚱 Internet Options 🛛 😝 Windows Firewall		Reference Options Automatic Updates
	Automatic Updates		Windows Firewall
t Microsoft, we care about your privacy	/. Please read our <u>privacy statement</u> .		•
a microsoft, we care about your privacy	. Peace read out gridges stategoes.		
Y ACADEMY	Automatic Updates		S Wardows Frewall
cademy.com	🔓 brenne Opana 🧑 Wadow Frewal		🕐 Internet Options 🐁 Automatic Optiates
icuaciny.com			

FRAUDTOOLS: XP ANTIVIRUS The Great Finale



PEOPLE WHO FELL VICTIM

to this manipulation and registered a copy of XP Antivirus were in for a nasty surprise: instead of paying 39.95 dollars they were charged from 89.20\$ up to even 400\$

			2008			
USD 39.9	5					
Scanner + Spy PRICE: USD39	ware Remover + 1 9.95 (This is a One	Real-Time Time Onl	1 year free updat e Protection + bonu y Charge, your cred RADES FOR FREE!)	is features		
First name*:		1	Card type":	VISA / Visa Electron	-	
Last name":			Card number*:			
Cardholder name":				(no spaces, no dashes, i.e. 41001	11100001111)	
Zip (Postal code)":			cvv*:			
Street*:			Expiration date :	2008 🗙 / 01 💌		
City*:						
Country":	United States	~	Customer service phone:			
				BUY		
Email": Phone:				s marked with " sign are re		



FRAUDTOOLS: XP ANTIVIRUS The Great Finale



THERE WERE VERY MANY others like this one





www.SecAcademy.com

THANKS



