Compte-rendu

Présentation pour le groupe OSSIR Paris
10/11/2009

Saâd Kadhi -- HAPSIS

Agenda

★ Présentation générale

★ Improvisation et Lightning talks

★ Workshops

★ Surface d'attague 2.0

★ Surface d'attague 1.0

★ Conclusion

Présentation Générale

Informations Générales

★ Conférence dédiée à la sécurité

★ Durée : 3 jours

★ Lieu : Grand Duché du Luxembourg

★ 5ème édition, 170 inscriptions env.

Programme

★ 1er jour : Workshops

★ 2ème et 3ème jours : Présentations, Improvisation et Lightning Talks

★ 7 workshops, 14 présentations

Ressenti

★ Très bonne organisation (avec quelques imprévus...)

★ Excellente ambiance

★ Pas de multiples tracks (sauf pour les workshops)

★ Présentations de bonne qualité en général

Improvisations et Lightning Talks

Improvisations

★ D'un côté : Des volontaires (pas toujours...)

★ De l'autre : Des présentations qu'ils n'ont jamais vu

★ C'est comme le Free Jazz (on aime ou pas)

Les sujets

★ Pimps and Hip-Hop

★ Grey's Anatomy

★ States of Mind

★ The Secrets of Quantum Crypto

★ Chicken Chicken Chicken

Lightning Talks

★ Windows 7: ROT13 or Vigenere? ;-)

★ iAWACS2009 feedback (Anti-virus "PWN2RM" Challenge Results)

★ Some news of TCP and IP security at IETF

★ Origami in PDF

★ Some Tools You Might Find Useful

Windows 7: ROT13 or Vigenere? ;-)

Didier Stevens

★ UserAssist: Infos sur les programmes les plus couramment appelés

★ Stockées "chiffrées" dans le re

★ Algorithme : ROT13 puis Vigener partir de Windows 7 / 2008 R2

Le sys continue de stocker les infos même quand l'option est désactivée

Vigenere uniquement pour les beta builds pour "faciliter" les tests

iAWACS2009 feedback (Anti-virus "PWN2RM" Challenge Results)

Eric Filliol, Anthony Desnos

★ Désactivation d'AV "on-the-fly"

★ Règles du concours publiées 2 mois à l'avance

★ 7 AV testés

★ Utilisation du test standard EICAR pour prouver la désactivation (pas de Reverse Engineering ou de malware)

iAWACS2009 ... (continued)

- ★ McAfee : 2 mins (SYSTEM)
- ★ Symantec : suppression des signatures
- ★ NOD32, Kaspersky, AVG : \Device\PhysicalMemory (XP)
- ★ G-DATA : désactivation du pilote
- ★ Seul Dr. Web a résisté

Some news of TCP and IP security at IETF

Fernando Gont

★ Security Assessment of TCP draft, adopté par l'IETF (TCPM WG)

★ Security Assessment of IPv4 draft, adopté par l'IETF (OPSEC WG)

★ Security Implications of NAT, pas encore adopté par l'IETF

Origami in PDF

Guillaume Delugre

★ Framework en Ruby pour manipuler les PDFs et les rendre malicieux

★ Exemple d'un PDF qui embarque un client IRC (!)

Some Tools You Might Find Useful

Moxie Marlinspike

★ Port knocking : Rappels et problèmes

★ Séquence capturable/rejouable

★ Solution? Large choix de séquences, crypto

★ Et là, tout le monde a perdu l'esprit...

Some Tools You Might ... (continued)

★ Or le but est de réduire le code exposé, pas l'augmenter

★ Knockknock: envoi d'un seul pagu SYN à un port fermé

★ Message IND-CPA

★ outil très simple, en Python, séparation de privilèges

Indistinguishability under chosen plaintext attack

15 lignes de code en root


HACK
.LU
09
HACK.LU is an open conference
where people can discuss
about computer security, privacy,
information technology and its
cultural/technical implication on society.
28-30
October

Workshops

7 Workshops

- ★ DAVIX - Visualization Workshop
- ★ Identifying security weaknesses in your VoIP systems
- ★ Advanced Network Based IPS Evasion Techniques
- ★ OWASP Luxembourg - Owning your network with just one phone call
- ★ Bypassing the Perimeter: Client Side Exploitation
- ★ Soldering: How not to burn your fingers
- ★ The Traveling Hacksmith

Davix Visualisation Workshop

Jan P. Monsch

★ Introduction à la visualisation appliquée à la sécurité des S.I.

★ Champ d'application relativement jeune

★ Quelques outils avec des formats/ interfaces différentes ...

Davix Visualisation... (continued)

★ DAVIX, Distro Linux (Live CD) spécialisée dans ce domaine

★ Manuel de 128 pages

★ Capturer, enregistrer, visualiser

★ Exercices et exemples avec des captures réelles

Bypassing the Perimeter: Client Side Exploitation

Nitesh Dhanjani, Billy K Rios

★ Différentes techniques pour exploiter les navigateurs (iPhone compris)

★ Pas de workshop, juste une présentation (problème de VM)

★ Compromission puis récupération de la base de mots de passe FireFox

Bypassing the Perimeter... (continued)

★ Base sous sqlite depuis FF 3.5.
Outils pour la cracker disponibles

★ Application FaceBook pour iPhone:
HTTP sans cookie, multipart.
Capture et rejeu et hop!

★ Beaucoup d'applications iPhone
présentent ces faiblesses

Bypassing the Perimeter... (continued)

- ★ Utilisation d'un PDF malicieux et Foxit Reader pour exécuter des commandes système
- ★ XSS dans Safari via feed:// (insertion JS dans tag <summary>
- ★ Menu alléchant mais on reste sur sa faim...

Surface d'Attaque 2.0

Qui dit 2.0 dit navigateur

★ Plusieurs présentations se sont intéressées de près à l'exploitation du navigateur ou de ses plugins

★ Périmètre ? Quel périmètre ?

★ Le navigateur n'est-il pas le nouvel OS d'aujourd'hui (avec la sécurité des OS d'il y a 10 ans) ?

Fun with Firefox Extension Malware

Candid Wuest

★ Sécurité Extensions FF ~= Sécurité ActiveX

★ Codées en Javascript, C++, ...

★ Installables n'importe où sur le système

Fun with Firefox... (continued)

★ Distribuées au format XPI, souvent non signées (pas de problème)

★ FF 3.X, 22% du marché

★ 170 millions d'extensions téléchargées / jour

★ 150 nouvelles / jour, 450 mises à jour quotidiennement

Fun with Firefox... (continued)

★ Une extension peut faire tout ce que FF peut faire : contrôle de l'UI, ...

★ Cocktail JavaScript pour manipuler Chrome? Game Over!

★ Exemples d'incidents réels : NoS
et Adblock Plus, pack linguistiq
namien vérolé,
ojan.ChromeInject

Mozilla utilise ClamAV, qui n'a pas détecté le virus.

Vol d'identifiants pour sites financier, cache son existence, ...

Fun with Firefox... (continued)

★ Une extension peut être installée furtivement par un malware

★ Sans oublier l'effet social ~~networkingengineering~~

★ Il existe plusieurs façons d'installer une extension

Fun with Firefox... (continued)

★ Tag "hidden" ou add-on type = 0 dans install.rdf,

★ modification runtime de la liste d'extensions,

★ modification de extension.rdf après installation,

★ hijack d'extensions existantes (même signées), hijack de fichiers FF...

Fun with Firefox... (continued)

★ Démo très convaincante

★ Ajout de cookies de tracking, redirection transparente vers des sites malicieux

★ backdoor (get clipboard, browse local FS, get FF profile, upload/execute file, registry navigator r/w, ...)

Fun with Firefox... (continued)

★ Extensions FF très puissantes

★ La plupart des AV actuels ne les vérifient pas

★ N'oublions pas GreaseMonkey et les User Scripts

★ "There is no best browser"

PDF (Penetration Document Format) + Malicious PDF Origamis Strike Back

Didier Stevens, Fred Raynal, Guillaume Delugre

★ Adobe Reader embarque un interpréteur Javascript

★ PDF + JavaScript = cocktail explosif

★ Création de PDF malicieux (et fort dangeureux) et signés avec la clé privée d'Adobe !

PDF (Penetration Document ... (continued)

★ Clé privée d'Adobe récupérée depuis un des produits de l'entreprise (reverse engineering ?)

★ Adobe Reader 9.1, une surface d'attaque impressionnante : 300 MB, 100 DLLs et exécutables

★ Virus PDF, auto-réplication

PDF (Penetration Document ... (continued)

★ Insertion d'un EICAR dans un PDF.
Seuls 5 AV sur 41 le détectent

★ Même test avec EICAR en ASCIIHexDecode : 2/41...

★ EICAR dans PDF chiffré avec mot de passe à blanc : 1/41

PDF (Penetration Document ... (continued)

★ Actions JavaScript dans PDF : / JavaScript (peut être obfusqué)

★ PDFiD, outil d'aide à la détecti PDF malicieux

★ Utilisé par VirusTotal et Nautilus (GNOME)

VirusTotal envoie tous les échantillons qu'il reçoit aux vendeurs d'AV

PDF (Penetration Document ... (continued)

★ Framework Origami inclut un outil assez similaire (pdfscan.rb)

★ Mais Origami est plus adapté à l'attague (création de PDF malicieux)

★ Attague typique : open PDF, exec JS, exploit JS, shellcode, exec trojan

PDF (Penetration Document ... (continued)

★ Autre possibilité : open PDF, exploit PDF, shellcode, exec trojan

★ Démo : SMB relay attack via PDF

★ SMB relay (Metasploit), PDF malicieux -> Envoi d'identifiants et John The Ripper

★ Adobe Reader ne donne aucun warning

PDF (Penetration Document ... (continued)

★ Comment se protéger ?

★ Foxit Reader ? N'y pensez même pas

★ Sumatra PDF (pas de JS)

★ Désactiver JS dans Adobe Reader
mais fenêtre d'alerte à chaque
ouverture avec "activer" sélectionné
par défaut ...

PDF (Penetration Document ... (continued)

★ Utilisation de PDFiD

★ Les comportements doivent évoluer

★ PDF est encore vu comme un "simple" document

Owage 2.0

Saumil Shah

★ Rappels des différentes manières pour l'exploitation client-side

★ Constat : " Users want to click, not think"

★ La surface d'attague est énorme

Ownage 2.0 (continued)

★ Et dire que HTML 5 et ses codecs embarqués sera bientôt là

★ " If you sneeze, there`s a JS event for it, if your eye goes to the top left corner, again there`s a JS event"

★ Les plug-ins sont une très bonne porte d`entrée

Ownage 2.0 (continued)

★ Sans oublier PDF qui attire beaucoup d`attention ces derniers temps

★ ... ou JS, Java, Flash, VBA...

★ Il est possible de créér des "paquetages" d`attaques utilisant les extensions, les plug-ins, toolbars, etc.

Ownage 2.0 (continued)

★ Exemple avec la Yahoo! toolbar : lancement d'une recherche sans interaction utilisateur

★ Exemple de corruption mémoire IE7 et ouverture de backdoor

★ Mais comment "livrer" les attaques ?

Ownage 2.0 (continued)

★ Nous vivons à l'époque de Google, FaceBook et Twitter

★ URLs shorteners (bit.ly, tinyurl)

★ Contournement de same-origin policy via les sites qui offrent un "print.asp?url=http" (inurl:...)

Ownage 2.0 (continued)

★ Injection SQL massive en cherchant les .asp et les URLS qui contiennent un a=...

★ Passage par un PDF malicieux contenant du Javascript obfusqué

★ Très bonne méthode pour contourner les AV

Ownage 2.0 (continued)

★ Démo avec une toolbar "cachée" à l'intérieur d'un PDF malicieux qui s'installe dans IE7 silencieusement et qui capture automatiquement toutes les pages naviguées, les mots de passe etc.

★ Futur champ d'investigation : les URLS de type "data://javascript/..."

More Tricks for Defeating SSL in Practice

Moxie Marlinspike

★ "Réchauffé" de Black Hat US 09

★ Attaques très élégantes contre SSL et plus exactement la vérification de certificats

★ Voir CR Black Hat US de HSC présenté à l'OSSIR en Septembre

★ Quelques moments forts à noter

More Tricks for Defeating... (continued)

★ Ne pas oublier que la plupart des utilisateurs cliquent sans penser

★ sslstrip remplace les liens HTTPS par leurs équivalents HTTP

★ Remplacement de favicon.ico par un cadenas ;-)

More Tricks for Defeating... (continued)

★ Une preuve que sslstrip marche ?

★ Exécution sur le réseau wifi hack.lu durant la présentation "Ownage 2.0" (env. 45 minutes)

★ 12 utilisateurs/mots de passe récupérés

★ Ah et OCSP peut être entièrement vaincu par le chiffre "3" (retry later)

Surface d'Attaque î.0

N'oublions pas le "i.0" ...

★ Quelques présentations plus "classiques"

★ MS Office, Delphi/Pascal, OS Fingerprinting, réseaux sans-fil, fuzzing...

Analyzing Word and Excel Encryption

Eric Filiol -- Rescue Keynote

★ Une bonne dose de crypto pour ouvrir la conférence

★ Travaux sur le déchiffrement de documents Word/Excel protégés par mot de passe

★ Les méthodes de chiffrement utilisent du XOR (!) ou du RC4

Analyzing Word and... (continued)

★ Attaque opérationnelle contre documents Word/Excel protégés, jusqu'à Office 2003 inclus

★ 91% de réussite. Utilise faiblesses Office et Windows

★ RC4 montre des faiblesses importantes lorsque la clé est < 2048 bits

Analyzing Word and... (continued)

★ Word/Excel 97/2000, clé de 40 bits

★ Word/Excel 2003, clé de 128 bits

★ Un fichier temporaire par révision

★ Effacement non sécurisé

★ Trap or not trap?

New advances in Office Malware analysis

Frank Boldewin

★ Méthodes d'analyse de malware pour MS Office

★ Pas d'exploitation connue du format XML

★ Travaux ciblés sur OLESS, à l'aide d'OfficeMalScanner Suite et d'OffVis

Fuzzgrind, an automatic fuzzing tool

Gabriel Campana

★ Rappels sur le fuzzing

★ Création de fuzzgrind à des fins d'automatisation

★ Basé sur Valgrind et STP

★ Nouvelles vulnérabilités découvertes dans libtiff par Tavis Ormandy

★ Résolution de quelques "crackme"

HostileWRT

Philippe Langlois, Eugene Parkinson

★ Plate-forme d'audit automatisé de réseaux sans-fil

★ Tente d'avoir accès à tous les réseaux sans-fil découverts

★ Dès qu'un réseau sans-fil est craqué, création d'un nouveau réseau "LoveWRT" pour bénéficier de l'accès

HostileWRT (continued)

★ "A neat but illegal way of getting around HADOPI"

★ Basé sur OpenWRT, hardware FON2 (50 €), programmé en ash

★ Plusieurs modes: auto-join on crack, mass audit (collect and crack)...

★ A venir : portails captifs

IpMorph: Unification of OS fingerprinting defeating

Florian Vichot, Guillaume Prigent

- ★ Mécanismes pour déjouer le fingerprinting d'OS aussi bien actif que passif
- ★ Protection de VM depuis un VM host
- ★ Modification à la volée de paquets sans dysfonctionnement réseau
- ★ Beta release 0.1 en juin 2009 (SSTIC)

Autres Présentations

- ★ Peeking into Pandora's Bochs - instrumenting a full system emulator to analyse malicious software
- ★ Perseus: A Coding Theory-based Firefox Plug-in to Counter Botnet Activity
- ★ Exploiting Delphi/Pascal
- ★ Some insights about the recent TCP DoS (Denial of Service) vulnerabilities
- ★ Implementation of K-ary Viruses in Python
- ★ Forensic and anti forensic enhancement with a H/VM virtual monitor
- ★ Playing in a satellite environment 1.2
- ★ When E.T. comes into Windows Mobile 6...


1305-17-109-9617 (17-A355)
1800 CARTRIDGE, 5.56 MM:
BLANK, NR 297C1
LOT IVI 98-7
10
UN 0014
CARTRIDGES, SMALL ARMS, B NK
UN 4A2/Y50/S/91/NL/
1.4
S
1

Conclusion

Client-side, quand tu nous tiens

★ Les navigateurs et les différents éléments avec lesquels ils interagissent (PDF, Office...) constituent une énorme surface d'attaque

★ Les outils de sécurité (AV notamment) actuels sont dépassés

Remerciements

★ OSSIR

★ HAPSIS

Informations Utiles

★ Vous pouvez télécharger cette présentation en ligne sur le site de l'OSSIR

★ Questions ? Commentaires ?

- saad.kadhi@hapsis.fr

Intervenant

★ Saâd Kadhi, consultant sécurité, HAPSIS (http://www.hapsis.fr/)

Licence

★ Creative Commons Attribution-NonCommercial 3.0

- http://creativecommons.org/licenses/by-nc/3.0/