Retour sur 10 ans d'audit sécurité

...

Menaces et protections : ce qui a changé

Jérémy Lebourdais (ON-X) - Renaud Feil (Synacktiv)

ON-X SÉCURITÉ NUMÉRIQUE

SYNACKTIV DIGITAL SECURITY

Résumer 10 années d'audit sécurité en 40 minutes...

- Retour vers le passé : 10 ans d'insécurité
- Évolution des menaces et des protections
- Succès et échecs d'aujourd'hui : la fracture de sécurité numérique
- Et les 10 prochaines années ?

Notre vision de l'évolution de la sécurité

Speakers

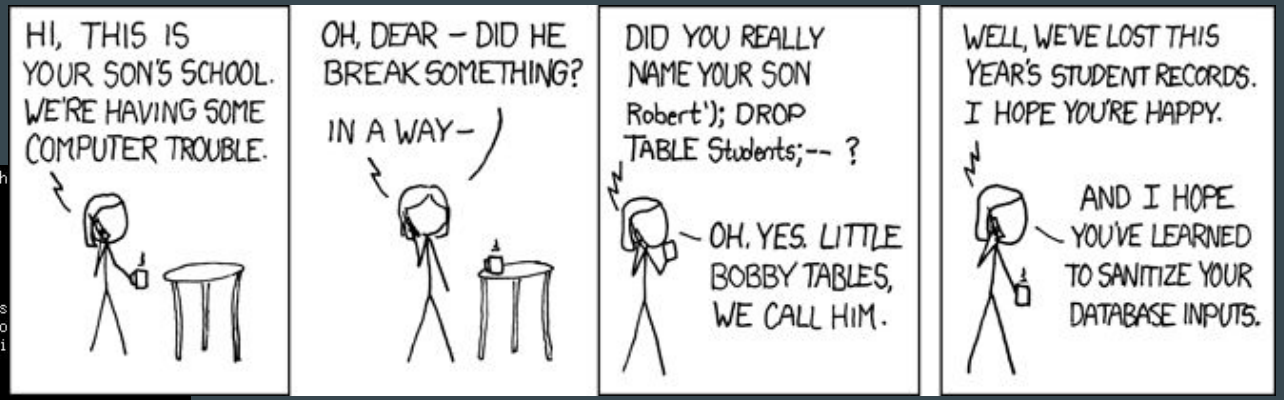
- Jérémy Lebourdais - Consultant senior chez ON-X Sécurité Numérique
  - Auditeur sécurité depuis janvier 2006
  - Passionné de sécurité, technophile, curieux de savoir “comment ça marche”
  - A réalisé de nombreux tests d’intrusion et audits

- Renaud Feil - Co-fondateur de Synacktiv
  - Auditeur sécurité depuis juillet 2005 (France et Australie)
  - Équipe francophone de CTF (*Capture The Flag*)
  - Suivi de nombreuses missions de tests d’intrusion et d’audits de sécurité

Retour vers le passé : 10 ans d’insécurité

L’insécurité des applications web

- Les injections SQL (et XSS) se trouvaient les yeux fermés
  - L’apostrophe et le guillemet étaient les rois




```
$ python sqlmap.py -u "http://target/vuln.php?id=1" --batch
                         {1.0-dev-4512258}
                         http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets
 consent is illegal. It is the end user's responsibility to
local, state and federal laws. Developers assume no liabili
sible for any misuse or damage caused by this program

[*] starting at 15:02:07

[15:02:07] [INFO] testing connection to the target URL
[15:02:07] [INFO] heuristics detected web page charset 'ascii'
[15:02:07] [INFO] testing if the target URL is stable. This can take a couple of
 seconds
[15:02:08] [INFO] target URL is stable
[15:02:08] [INFO] testing if GET parameter 'id' is dynamic
[15:02:08] [INFO] confirming that GET parameter 'id' is dynamic
[15:02:08] [INFO] GET parameter 'id' is dynamic
[15:02:08] [INFO] heuristic (basic) test shows that GET parameter 'id' might be
injectable (possible DBMS: 'MySQL')
```

- Débuts de SQLMap !

Exploitation massive des premières vulnérabilités dans les lecteurs de format

- Faille WMF fin 2005

Un patch "officieux" recommandé pour corriger une faille de Windows

Sécurité : *La faille affectant la librairie d'images WMF de Windows a été exploitée et fait de nombreuses victimes. Face à l'urgence, des experts en sécurité conseillent d'installer une rustine créée par un développeur tiers. En attendant le patch de Microsoft.*

Par Tom Espiner, ZDNet UK et Joris Evers, CNET News.com | Mercredi 04 Janvier 2006

Posted by Mikko @ 20:09 GMT

Microsoft WMF patch coming out today

We just got the word that Microsoft is going out of normal update cycle to release security update MS06-001 today. This will fix the WMF vulnerability on XP, 2003 and 2000 (sp4) systems.

Microsoft originally planned to release the update on next Tuesday, but they finished testing early.

Everybody was hoping they would get the patch out before a major attack would start. Now it looks like they succeeded in doing just that. Well done.

Update: The patch can now be downloaded from here. It seems to co-exist fine with the REGSVR32 workaround and the Ilfak patch.

Bulletin de sécurité Microsoft MS06-001 - Critique

Une vulnérabilité du moteur de rendu graphique pourrait permettre l'exécution de code à distance (912919)

Paru le: jeudi 5 janvier 2006

Version: 1.0

Synthèse

Personnes concernées par ce document : Les clients utilisant Microsoft Windows

Type de vulnérabilité : Exécution de code à distance

Indice de gravité maximal : Critique

Florilège de corruptions de mémoire exploitables à distance

- Exploitation massive de la vulnérabilité MS03-026

- L'outil Metasploit intègre l'exploit pour MS08-067

Évolution des menaces et des protections

Microsoft Trustworthy Computing

- SD3+C
  - Secure by Design
  - Secure by Default
  - Secure in Deployment
  - Communications
- Disparition progressive (mais lente) d'Internet Explorer 6
- Protections génériques contre l'exploitation des corruptions de mémoire
  - ASLR, DEP, /GS, Safe SEH, SEHOP, etc.
- Autres mécanismes de sécurité
  - AppLocker
  - Niveaux d'isolation

Mais toujours des surprises… quelques exemples…

- 2009 : nombreuses vulnérabilités dans SMBv2 par Laurent Gaffié… mais aucun exploit public…
- Mars 2016: réponse du MSRC à Synacktiv sur une vulnérabilité permettant le contournement d'AppLocker

Hello,

Thank you for contacting the Microsoft Security Response Center (MSRC). AppLocker is not a security boundary and we do not currently service issues related to it.

Again, we appreciate your report.

Regards,

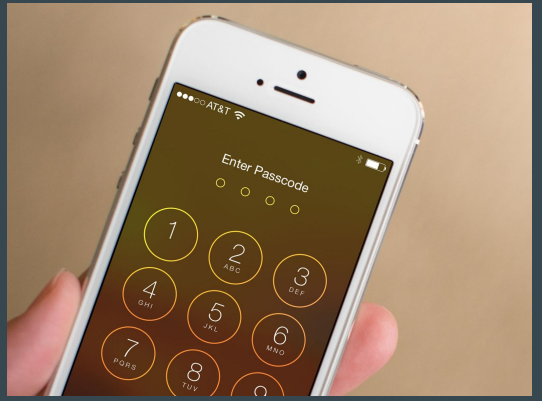
Jonathan
MSRC

Google

- Google Chrome
  - Sandbox
  - DPAPI
- Projet Zero
  - Attaque de produits d'autres éditeurs !
  - 90 jours pour la publication d'un correctif, avant divulgation
- Sandbox Native Client
  - Limite l'impact de l'évasion de la sandbox Python de Google AppEngine découverte par Synacktiv en 2014

La surprise Apple

- Succès sécurité pour iOS
  - Aveu de faiblesse du FBI
- La sécurité comme outil marketing
- Les effets de l'affaire Snowden : le gouvernement comme menace



- Mais encore des erreurs surprenantes

```
        hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
    hashOut.length = SSL_SHA1_DIGEST_LEN;
    if ((err = SSLFreeBuffer(&hashCtx)) != 0)
        goto fail;

    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;

        err = sslRawVerify(ctx,
                           ctx->peerPubKey,
                           dataToSign,                /* plaintext */
                           dataToSignLen,             /* plaintext length */
                           signature,
-uu-:---F1  sslKeyExchange.c   30% L602   (C/l Abbrev Isearch)----------------
I-search: goto fail
```

Succès et échecs d’aujourd’hui : la fracture de sécurité numérique

Une évolution certaine

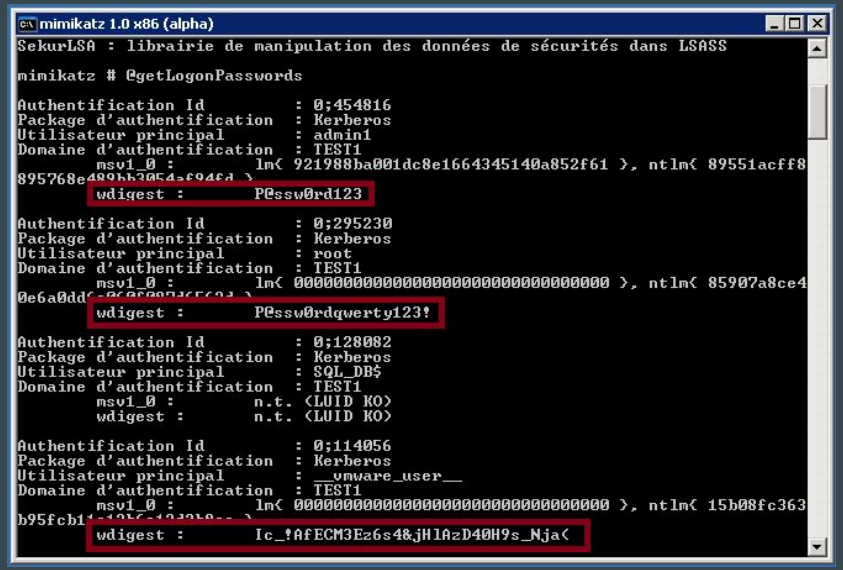
- Configurations par défaut renforcées
- Intégration de la sécurité dans les frameworks
- Désactivation de versions vulnérables de Flash dans Firefox, Chrome, idem pour Java
- Publication de correctifs à intervalles réguliers de Microsoft, Oracle, Adobe mais aussi Samsung pour Android
- OWASP: nombreux guides

Mais toujours des échecs...

- Heartbleed
  - Présent dans openSSL depuis fin 2011, découvert en 2014
  - Impacte les serveurs mais aussi les clients
- Android
  - Modèle intéressant
  - Mais de nombreuses erreurs d'implémentation.
  - Diversité des versions ⇒ corrections difficiles
  - Tapjacking, Towelroot, Stagefright, FakeId
- Cisco
  - Mots de passe Type 4 moins sûrs que le Type 5

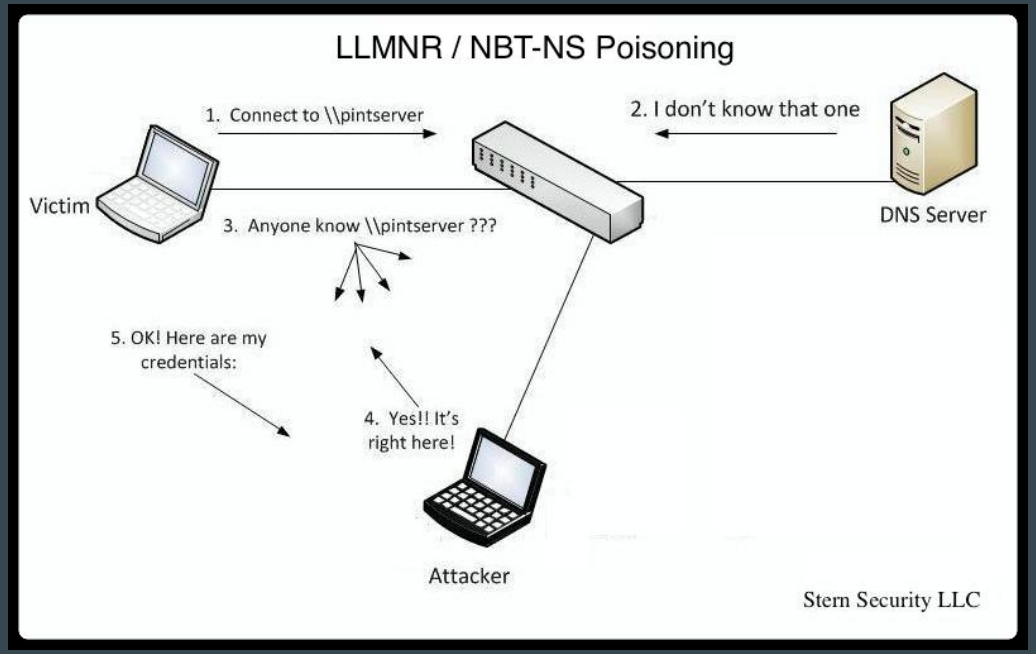
Microsoft Windows : le poids de l'héritage

- Algorithmes de hachage des mots de passe faibles
  - Disparition partielle du format LM
  - Puissance de calcul face au format NT (la plaie des mots de passe)
- Attaques de type *pass-the-hash* au coeur du protocole d'authentification NTLM
  - Le condensat du mot de passe est le secret !
- Le redoutable outil mimikatz



Sécuriser un réseau interne reste encore difficile

- Protocoles LLMNR, NBNS et WPAD
- L'outil Responder



Changement des stratégies d'attaques depuis Internet

- La porte d'entrée royale des macros dans les documents Office
- Les ransomwares
  - Cryptolocker, Dridex, etc.
  - Lourd impact auprès du grand public et des PME

Les failles techniques ne sont pas les seules

- L'importance du contrôle, et pas seulement pour les injections
  - Identification via un ID non contrôlé
  - Appel direct aux URL
- Données sensibles
  - Non identifiées ⇒ non protégées
  - Incorporées dans d'autres (fichier de sauvegarde ZIP) ⇒ perte de la sensibilité
- Difficulté de se tenir à jour
  - Qualification des correctifs / mises à jour
  - Impératifs liés à des applicatifs métier
- Importance réelle du "maillon le plus faible"
  - Nécessité de considérer la cible dans son ensemble
  - Souvent problématique pour des applications complexes

Et les 10 prochaines années ?

Le métier d'auditeur sécurité en constante évolution

- Prise de conscience des enjeux et hausse des budgets sécurité
- Encadrement croissant de la profession par l'ANSSI
- Spécialisation des sociétés de tests d'intrusion
  - Et des candidats au poste de pentester !
- Prestations réalistes type "Red Team"
  - cf hors-série MISC numéro 12
- Les Bug Bounty
  - Vers une "ubérisation" du métier ?

BOUNTY FACTORY.io

Évolution de la menace

- Compromission des tiers
  - Compromission de Target
  - XcodeGhost
  - Le cloud et l'illusion de la séparation entre clients
  - La multiplication des bibliothèques et des plugins tiers
  - La compromission des sources (Linux Mint)
- Menaces étatiques et professionnalisation
  - Hacking Team
  - Zerodium

]HackingTeam[

Évolution de la défense

- SOC et SIEM
  - Nécessité d'analyse globale
  - Pendant défensif de la Red Team (Blue Team)
  - Exercice difficile
- Cybersurveillance
- Protection de l'intégrité des données
- Défenses au plus près des systèmes (objets connectés)
- Fracture entre les bons élèves et les mauvais