

Ingénierie Sociale

Éric BERTHOMIER
eric.berthomier@free.fr

16 mars 2022



Introduction

L'ingénierie Sociale utilise l'influence et la persuasion pour **duper**, **convaincre** et **manipuler**.



Introduction

L'ingénierie Sociale utilise l'influence et la persuasion pour **duper**, **convaincre** et **manipuler**.

En conséquence, l'ingénierie sociale est capable de prendre avantage sur les gens pour obtenir des informations **avec ou sans** l'utilisation de technologies.

Ce cours est une adaptation de <https://www.stationx.net/>



Ce qui va suivre

Ce qui va suivre est un exemple d'audit effectué pour un client (États Unis).



Ce qui va suivre

Ce qui va suivre est un exemple d'audit effectué pour un client (États Unis).

Il démontre que ce qui peut sembler être des informations **insignifiantes** peut construire un climat de confiance avec les gens et compromettre ainsi une société.



Pour expliquer comment je vais associer l'ingénierie sociale à la technologie, il est nécessaire de vous expliquer les outils utilisés.



Pour expliquer comment je vais associer l'ingénierie sociale à la technologie, il est nécessaire de vous expliquer les outils utilisés.

Nous disposons de nombreux outils que nous avons développés à des fins de tests d'intrusion.



Pour expliquer comment je vais associer l'ingénierie sociale à la technologie, il est nécessaire de vous expliquer les outils utilisés.

Nous disposons de nombreux outils que nous avons développés à des fins de tests d'intrusion.

Dans l'exemple de l'ingénierie sociale, j'utiliserai un package ou "executable wrapper", un rootkit et un RAT (Remote Access Tool, Trojan).



En termes simples, le wrapper peut créer des programmes exécutables qui apparaissent comme faisant une tâche, mais, en fait, effectuant d'autres tâches dans le même temps.



En termes simples, le wrapper peut créer des programmes exécutables qui apparaissent comme faisant une tâche, mais, en fait, effectuant d'autres tâches dans le même temps.

Notre wrapper peut encrypter, et compresser le contenu d'un programme pour éviter la détection de virus et le forensic.



Le RAT est un outil de contrôle à distance qui, quand il fonctionne sur une machine, recherche des connexions réseaux pour se rendre sur l'Internet, en utilisant un proxy ou d'autres éléments au besoin.



RAT

Le RAT est un outil de contrôle à distance qui, quand il fonctionne sur une machine, recherche des connexions réseaux pour se rendre sur l'Internet, en utilisant un proxy ou d'autres éléments au besoin.

Le RAT utilise les connexions sortantes de la machine cible pour recevoir ses commandes afin de bypasser tout dispositif de sécurité tel qu'un firewall ou un NAT.



RAT

Le RAT est un outil de contrôle à distance qui, quand il fonctionne sur une machine, recherche des connexions réseaux pour se rendre sur l'Internet, en utilisant un proxy ou d'autres éléments au besoin.

Le RAT utilise les connexions sortantes de la machine cible pour recevoir ses commandes afin de bypasser tout dispositif de sécurité tel qu'un firewall ou un NAT.

Les communications sont envoyées au travers du trafic HTTP/HTTPs, donc même si le proxy ou le firewall de la cible dispose d'un filtrage au niveau applicatif, les commandes de contrôle apparaîtront comme un trafic réseau HTTP normal, car c'en est un !



Le RAT est un outil de contrôle à distance qui, quand il fonctionne sur une machine, recherche des connexions réseaux pour se rendre sur l'Internet, en utilisant un proxy ou d'autres éléments au besoin.

Le RAT utilise les connexions sortantes de la machine cible pour recevoir ses commandes afin de bypasser tout dispositif de sécurité tel qu'un firewall ou un NAT.

Les communications sont envoyées au travers du trafic HTTP/HTTPS, donc même si le proxy ou le firewall de la cible dispose d'un filtrage au niveau applicatif, les commandes de contrôle apparaîtront comme un trafic réseau HTTP normal, car c'en est un !

Ceci signifie que nous pouvons communiquer avec les cibles au travers des réseaux de l'entreprise sans se soucier des firewalls / proxies / DMZ , etc (puisque c'est le poste de l'utilisateur qui fait les



Rootkit

Le Rootkit est un programme qui camoufle les actions du hacker et ceci **contre le système d'exploitation** mais aussi **contre tout examen de la machine par un individu.**



Rootkit

Le Rootkit est un programme qui camoufle les actions du hacker et ceci **contre le système d'exploitation** mais aussi **contre tout examen de la machine par un individu**.

Notre rootkit camoufle des Processus, des Handles (point d'accès à des fichiers), des Modules, des Fichiers et des Répertoires, des Clés de Registre et ses valeurs, des Services, des sockets (connexions) TCP/UDP et des icônes de la Systray.



Rootkit

Le Rootkit est un programme qui camoufle les actions du hacker et ceci **contre le système d'exploitation** mais aussi **contre tout examen de la machine par un individu**.

Notre rootkit camoufle des Processus, des Handles (point d'accès à des fichiers), des Modules, des Fichiers et des Répertoires, des Clés de Registre et ses valeurs, des Services, des sockets (connexions) TCP/UDP et des icônes de la Systray.

Ceci signifie que le gestionnaire des tâches, netstat, regedit, explorer, etc. ne sont plus capables de voir ce qui se passe au niveau de la machine qui a été rootkité par le hacker.



Rootkit

Le Rootkit est un programme qui camoufle les actions du hacker et ceci **contre le système d'exploitation** mais aussi **contre tout examen de la machine par un individu**.

Notre rootkit camoufle des Processus, des Handles (point d'accès à des fichiers), des Modules, des Fichiers et des Répertoires, des Clés de Registre et ses valeurs, des Services, des sockets (connexions) TCP/UDP et des icônes de la Systray.

Ceci signifie que le gestionnaire des tâches, netstat, regedit, explorer, etc. ne sont plus capables de voir ce qui se passe au niveau de la machine qui a été rootkité par le hacker.

Les actions et les programmes du hackers seront alors invisibles.



Il existe des versions moins sophistiquées de ce type d'outils sur Internet mais il y a 2 bonnes raisons pour lesquelles un hacker professionnel ne les utilisera pas.



Il existe des versions moins sophistiquées de ce type d'outils sur Internet mais il y a 2 bonnes raisons pour lesquelles un hacker professionnel ne les utilisera pas.

- La première est qu'ils ne peuvent procurer l'ensemble des fonctionnalités nécessaires à l'attaque.



Il existe des versions moins sophistiquées de ce type d'outils sur Internet mais il y a 2 bonnes raisons pour lesquelles un hacker professionnel ne les utilisera pas.

- La première est qu'ils ne peuvent procurer l'ensemble des fonctionnalités nécessaires à l'attaque.
- La seconde raison est que de nombreux anti-virus connaissent la signature de ces derniers et peuvent donc les arrêter.



Il existe des versions moins sophistiquées de ce type d'outils sur Internet mais il y a 2 bonnes raisons pour lesquelles un hacker professionnel ne les utilisera pas.

- La première est qu'ils ne peuvent procurer l'ensemble des fonctionnalités nécessaires à l'attaque.
- La seconde raison est que de nombreux anti-virus connaissent la signature de ces derniers et peuvent donc les arrêter.

C'est là toute la différence entre un script kiddy et un hacker professionnel.



Infiltration : Premiers contacts

Appel à la Réception de l'entreprise avec mon téléphone mobile.



Infiltration : Premiers contacts

Appel à la Réception de l'entreprise avec mon téléphone mobile.
– *Nathan* : Bonjour, j'ai un problème avec mon téléphone de bureau. Pourriez-vous me passer quelqu'un qui pourrait m'aider ?



Infiltration : Premiers contacts

Appel à la Réception de l'entreprise avec mon téléphone mobile.

– *Nathan* : Bonjour, j'ai un problème avec mon téléphone de bureau. Pourriez-vous me passer quelqu'un qui pourrait m'aider ?

– *Réception* : Je vous transfère.



Infiltration : Premiers contacts

Appel à la Réception de l'entreprise avec mon téléphone mobile.

– *Nathan* : Bonjour, j'ai un problème avec mon téléphone de bureau. Pourriez-vous me passer quelqu'un qui pourrait m'aider ?

– *Réception* : Je vous transfère.

– *ISC* : Bonjour



Infiltration : Premiers contacts

Appel à la Réception de l'entreprise avec mon téléphone mobile.

– *Nathan* : Bonjour, j'ai un problème avec mon téléphone de bureau. Pourriez-vous me passer quelqu'un qui pourrait m'aider ?

– *Réception* : Je vous transfère.

– *ISC* : Bonjour

– *Nathan* : Bonjour, j'ai un problème avec mon téléphone de bureau. Désolé je suis nouveau ici. Serait-il possible de savoir qui m'a appelé sur mon téléphone ? Est-ce qu'il existe une identification des appels ?



Infiltration : Premiers contacts

Appel à la Réception de l'entreprise avec mon téléphone mobile.

– *Nathan* : Bonjour, j'ai un problème avec mon téléphone de bureau. Pourriez-vous me passer quelqu'un qui pourrait m'aider ?

– *Réception* : Je vous transfère.

– *ISC* : Bonjour

– *Nathan* : Bonjour, j'ai un problème avec mon téléphone de bureau. Désolé je suis nouveau ici. Serait-il possible de savoir qui m'a appelé sur mon téléphone ? Est-ce qu'il existe une identification des appels ?

– *ISC* : Pas véritablement, du fait que nous utilisons des bureaux partagés. La plupart des gens utilisent souvent leur téléphone mobile, le numéro de l'appel n'est donc pas associé à un nom. Est-ce un problème pour vous ?



Infiltration : Premiers contacts

Appel à la Réception de l'entreprise avec mon téléphone mobile.

– *Nathan* : Bonjour, j'ai un problème avec mon téléphone de bureau. Pourriez-vous me passer quelqu'un qui pourrait m'aider ?

– *Réception* : Je vous transfère.

– *ISC* : Bonjour

– *Nathan* : Bonjour, j'ai un problème avec mon téléphone de bureau. Désolé je suis nouveau ici. Serait-il possible de savoir qui m'a appelé sur mon téléphone ? Est-ce qu'il existe une identification des appels ?

– *ISC* : Pas véritablement, du fait que nous utilisons des bureaux partagés. La plupart des gens utilisent souvent leur téléphone mobile, le numéro de l'appel n'est donc pas associé à un nom. Est-ce un problème pour vous ?

– *Nathan* : Non c'est bon, je comprends. Merci. Au revoir.



Conclusion

Je sais maintenant que la société utilise des bureaux partagés et que le numéro de l'appelant nest pas identifiable.



Conclusion

Je sais maintenant que la société utilise des bureaux partagés et que le numéro de l'appelant nest pas identifiable.

Donc ce nest pas un problème si jappelle de l'extérieur de la société.



Conclusion

Je sais maintenant que la société utilise des bureaux partagés et que le numéro de l'appelant n'est pas identifiable.

Donc ce n'est pas un problème si j'appelle de l'extérieur de la société.

Si cela avait été nécessaire, j'aurais dû contourner ce problème.



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?
- *Réception* : Très bien



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?
- *Réception* : Très bien
- *PC Sécurité* : Bonjour, en quoi puis-je vous aider ?



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?
- *Réception* : Très bien
- *PC Sécurité* : Bonjour, en quoi puis-je vous aider ?
- *Nathan* : Bonjour, je ne sais pas si cela vous intéressera mais j'ai trouvé une carte d'accès à l'extérieur du bâtiment. Certainement quelqu'un qui a dû la laisser tomber.



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?
- *Réception* : Très bien
- *PC Sécurité* : Bonjour, en quoi puis-je vous aider ?
- *Nathan* : Bonjour, je ne sais pas si cela vous intéressera mais j'ai trouvé une carte d'accès à l'extérieur du bâtiment. Certainement quelqu'un qui a du la laisser tomber.
- *PC Sécurité* : Ramenez nous la simplement. Nous sommes au bâtiment 3.



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?
- *Réception* : Très bien
- *PC Sécurité* : Bonjour, en quoi puis-je vous aider ?
- *Nathan* : Bonjour, je ne sais pas si cela vous intéressera mais j'ai trouvé une carte d'accès à l'extérieur du bâtiment. Certainement quelqu'un qui a dû la laisser tomber.
- *PC Sécurité* : Ramenez nous la simplement. Nous sommes au bâtiment 3.
- *Nathan* : Ok aucun problème. Qui dois-je demander ?



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?
- *Réception* : Très bien
- *PC Sécurité* : Bonjour, en quoi puis-je vous aider ?
- *Nathan* : Bonjour, je ne sais pas si cela vous intéressera mais j'ai trouvé une carte d'accès à l'extérieur du bâtiment. Certainement quelqu'un qui a dû la laisser tomber.
- *PC Sécurité* : Ramenez nous la simplement. Nous sommes au bâtiment 3.
- *Nathan* : Ok aucun problème. Qui dois-je demander ?
- *PC Sécurité* : Mon nom est Eric Wood, si je ne suis pas là, donnez le à Neil.



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?
- *Réception* : Très bien
- *PC Sécurité* : Bonjour, en quoi puis-je vous aider ?
- *Nathan* : Bonjour, je ne sais pas si cela vous intéressera mais j'ai trouvé une carte d'accès à l'extérieur du bâtiment. Certainement quelqu'un qui a dû la laisser tomber.
- *PC Sécurité* : Ramenez nous la simplement. Nous sommes au bâtiment 3.
- *Nathan* : Ok aucun problème. Qui dois-je demander ?
- *PC Sécurité* : Mon nom est Eric Wood, si je ne suis pas là, donnez-le à Neil.
- *Nathan* : Ok c'est noté. Je le ferai. Êtes-vous le responsable de la sécurité du bâtiment ?



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?
- *Réception* : Très bien
- *PC Sécurité* : Bonjour, en quoi puis-je vous aider ?
- *Nathan* : Bonjour, je ne sais pas si cela vous intéressera mais j'ai trouvé une carte d'accès à l'extérieur du bâtiment. Certainement quelqu'un qui a dû la laisser tomber.
- *PC Sécurité* : Ramenez nous la simplement. Nous sommes au bâtiment 3.
- *Nathan* : Ok aucun problème. Qui dois-je demander ?
- *PC Sécurité* : Mon nom est Eric Wood, si je ne suis pas là, donnez-le à Neil.
- *Nathan* : Ok c'est noté. Je le ferai. Êtes-vous le responsable de la sécurité du bâtiment ?
- *PCI* : Notre service est le service de "Contrôle des accès". Son directeur est Peter Reed.



Infiltration : Recherche de situation

- *Nathan* : Bonjour, puis-je avoir la sécurité des bâtiments ?
- *Réception* : Très bien
- *PC Sécurité* : Bonjour, en quoi puis-je vous aider ?
- *Nathan* : Bonjour, je ne sais pas si cela vous intéressera mais j'ai trouvé une carte d'accès à l'extérieur du bâtiment. Certainement quelqu'un qui a dû la laisser tomber.
- *PC Sécurité* : Ramenez nous la simplement. Nous sommes au bâtiment 3.
- *Nathan* : Ok aucun problème. Qui dois-je demander ?
- *PC Sécurité* : Mon nom est Eric Wood, si je ne suis pas là, donnez le à Neil.
- *Nathan* : Ok c'est noté. Je le ferai. Etes-vous le responsable de la sécurité du bâtiment ?
- *PCI* : Notre service est le service de "Contrôle des accès". Son directeur est Peter Reed.
- *Nathan* : Ok, merci. Au revoir.



Conclusion

Cet appel ma permis de connaître le nom dun membre du personnel de la sécurité, le nom correct du département, le responsable de la sécurité et sils sont responsables des cartes d'accès.



Recherche de la cible : Ressources Humaines (1/2)

– *Nathan* : Bonjour, j'appelle de la part d'un groupe de l'agence et j'aimerais savoir si quelqu'un pourrait m'aider. J'ai en effet un meeting à organiser dans 1 mois avec des personnes du RH mais par malchance mon ordinateur a crashé et j'ai perdu leurs noms.



Recherche de la cible : Ressources Humaines (1/2)

- *Nathan* : Bonjour, j'appelle de la part d'un groupe de l'agence et j'aimerais savoir si quelqu'un pourrait m'aider. J'ai en effet un meeting à organiser dans 1 mois avec des personnes du RH mais par malchance mon ordinateur a crashé et j'ai perdu leurs noms.
- *Réception* : Bien sûr aucun problème. Laissez-moi rechercher le département RH. Avez-vous une idée des noms ?



Recherche de la cible : Ressources Humaines (1/2)

- *Nathan* : Bonjour, j'appelle de la part d'un groupe de l'agence et j'aimerais savoir si quelqu'un pourrait m'aider. J'ai en effet un meeting à organiser dans 1 mois avec des personnes du RH mais par malchance mon ordinateur a crashé et j'ai perdu leurs noms.
- *Réception* : Bien sûr aucun problème. Laissez-moi rechercher le département RH. Avez-vous une idée des noms ?
- *Nathan* : Je sais que l'un d'entre eux était le responsable du pôle RH. Il y avait énormément de monde prévu à ce meeting.



Recherche de la cible : Ressources Humaines (1/2)

- *Nathan* : Bonjour, j'appelle de la part d'un groupe de l'agence et j'aimerais savoir si quelqu'un pourrait m'aider. J'ai en effet un meeting à organiser dans 1 mois avec des personnes du RH mais par malchance mon ordinateur a crashé et j'ai perdu leurs noms.
- *Réception* : Bien sûr aucun problème. Laissez-moi rechercher le département RH. Avez-vous une idée des noms ?
- *Nathan* : Je sais que l'un d'entre eux était le responsable du pôle RH. Il y avait énormément de monde prévu à ce meeting.
- *Réception* : ... Ok j'y suis. Le responsable du pôle RH est Marry Killmister ; 0207 *****



Recherche de la cible : Ressources Humaines (2/2)

– *Nathan* : Oui ça sonne bien. Avez vous dautres noms à me proposer dans les RH ?



Recherche de la cible : Ressources Humaines (2/2)

- *Nathan* : Oui ça sonne bien. Avez vous d'autres noms à me proposer dans les RH ?
- *Réception* : Au pôle *RH* : Jane Ross, Emma Jones. . .



Recherche de la cible : Ressources Humaines (2/2)

- *Nathan* : Oui ça sonne bien. Avez vous d'autres noms à me proposer dans les RH ?
- *Réception* : Au pôle *RH* : Jane Ross, Emma Jones. . .
- *Nathan* : Oui, je suis sûr pour Jane et Emma. Pourrais-je avoir leur téléphone ?



Recherche de la cible : Ressources Humaines (2/2)

- *Nathan* : Oui ça sonne bien. Avez vous dautres noms à me proposer dans les RH ?
- *Réception* : Au pôle *RH* : Jane Ross, Emma Jones. . .
- *Nathan* : Oui, je suis sûr pour Jane et Emma. Pourrais-je avoir leur téléphone ?
- *Réception* : Bien sûr : Jane Ross au ***** et Emma Jones au ***** . Souhaitez-vous que je vous mette en relation avec lune delles ?



Recherche de la cible : Ressources Humaines (2/2)

- *Nathan* : Oui ça sonne bien. Avez vous d'autres noms à me proposer dans les RH ?
- *Réception* : Au pôle *RH* : Jane Ross, Emma Jones. . .
- *Nathan* : Oui, je suis sûr pour Jane et Emma. Pourrais-je avoir leur téléphone ?
- *Réception* : Bien sûr : Jane Ross au ***** et Emma Jones au ***** . Souhaitez-vous que je vous mette en relation avec lune d'elles ?
- *Nathan* : Oui pouvez-vous me mettre en relation avec Emma s'il vous plait ?



Conclusion

Je connais maintenant trois personnes du pôle RH, dont le responsable de ce dernier.



Ingénierie Sociale - Ressources Humaines (1/2)

– *RH* : Bonjour Emma à l'appareil.



- *RH* : Bonjour Emma à l'appareil.
- *Nathan* : Bonjour Emma, cest Éric, du FS dans le bâtiment 3. J'espère que vous pourrez m'aider. Nous avons un problème ici avec la base des cartes d'accès. Elle a crashé la nuit dernière et certaines données concernant les nouveaux arrivants sont perdues. Sauriez-vous qui peut me dire qui sont les arrivants dans les deux dernières semaines sinon leur carte d'accès ne fonctionnera plus ? Nous avons besoin de les contacter rapidement.



- *RH* : Bonjour Emma à l'appareil.
- *Nathan* : Bonjour Emma, cest Éric, du FS dans le bâtiment 3. J'espère que vous pourrez m'aider. Nous avons un problème ici avec la base des cartes d'accès. Elle a crashé la nuit dernière et certaines données concernant les nouveaux arrivants sont perdues. Sauriez-vous qui peut me dire qui sont les arrivants dans les deux dernières semaines sinon leur carte d'accès ne fonctionnera plus ? Nous avons besoin de les contacter rapidement.
- *Emma* : Je peux vous aider. Je vais regarder les noms et je vous les envoie par mail si cela vous convient ? Pour les deux dernières semaines vous m'avez dit ?



- *RH* : Bonjour Emma à l'appareil.
- *Nathan* : Bonjour Emma, cest Éric, du FS dans le bâtiment 3. J'espère que vous pourrez m'aider. Nous avons un problème ici avec la base des cartes d'accès. Elle a crashé la nuit dernière et certaines données concernant les nouveaux arrivants sont perdues. Sauriez-vous qui peut me dire qui sont les arrivants dans les deux dernières semaines sinon leur carte d'accès ne fonctionnera plus ? Nous avons besoin de les contacter rapidement.
- *Emma* : Je peux vous aider. Je vais regarder les noms et je vous les envoie par mail si cela vous convient ? Pour les deux dernières semaines vous m'avez dit ?
- *Nathan* : Pour les deux dernières semaines en effet. Très bien, merci, mais serait-il possible de me le faxer, nous partageons un ordinateur pour les mails et ce dernier a crashé aussi.



- *RH* : Bonjour Emma à l'appareil.
- *Nathan* : Bonjour Emma, cest Éric, du FS dans le bâtiment 3. Jespère que vous pourrez m'aider. Nous avons un problème ici avec la base des cartes d'accès. Elle a crashé la nuit dernière et certaines données concernant les nouveaux arrivants sont perdues. Sauriez-vous qui peut me dire qui sont les arrivants dans les deux dernières semaines sinon leur carte d'accès ne fonctionnera plus ? Nous avons besoin de les contacter rapidement.
- *Emma* : Je peux vous aider. Je vais regarder les noms et je vous les envoie par mail si cela vous convient ? Pour les deux dernières semaines vous m'avez dit ?
- *Nathan* : Pour les deux dernières semaines en effet. Très bien, merci, mais serait-il possible de me le faxer, nous partageons un ordinateur pour les mails et ce dernier a crashé aussi.
- *Emma* : Oui, quel est votre numéro de fax ? Oh, et quel est votre nom déjà ?



- *RH* : Bonjour Emma à l'appareil.
- *Nathan* : Bonjour Emma, cest Éric, du FS dans le bâtiment 3. J'espère que vous pourrez m'aider. Nous avons un problème ici avec la base des cartes d'accès. Elle a crashé la nuit dernière et certaines données concernant les nouveaux arrivants sont perdues. Sauriez-vous qui peut me dire qui sont les arrivants dans les deux dernières semaines sinon leur carte d'accès ne fonctionnera plus ? Nous avons besoin de les contacter rapidement.
- *Emma* : Je peux vous aider. Je vais regarder les noms et je vous les envoie par mail si cela vous convient ? Pour les deux dernières semaines vous m'avez dit ?
- *Nathan* : Pour les deux dernières semaines en effet. Très bien, merci, mais serait-il possible de me le faxer, nous partageons un ordinateur pour les mails et ce dernier a crashé aussi.
- *Emma* : Oui, quel est votre numéro de fax ? Oh, et quel est votre nom déjà ?
- *Nathan* : Mettez le fax à l'attention de Eric. Je vais chercher le



– *Emma* : ok



- *Emma* : ok
- *Nathan* : Pourriez vous m'indiquer le temps nécessaire pour trouver linformation ?



- *Emma* : ok
- *Nathan* : Pourriez vous m'indiquer le temps nécessaire pour trouver linformation ?
- *Emma* : Ça ne devrait pas prendre plus de 30 minutes.



- *Emma* : ok
- *Nathan* : Pourriez vous m'indiquer le temps nécessaire pour trouver linformation ?
- *Emma* : Ça ne devrait pas prendre plus de 30 minutes.
- *Nathan* : Pouvez-vous commencer la recherche immédiatement ?
Cest très urgent.



- *Emma* : ok
- *Nathan* : Pourriez vous m'indiquer le temps nécessaire pour trouver linformation ?
- *Emma* : Ça ne devrait pas prendre plus de 30 minutes.
- *Nathan* : Pouvez-vous commencer la recherche immédiatement ? Cest très urgent.
- *Emma* : J'ai quelques petites choses à faire ce matin mais je vous communiquerai les noms dans laprès-midi.



- *Emma* : ok
- *Nathan* : Pourriez vous m'indiquer le temps nécessaire pour trouver linformation ?
- *Emma* : Ça ne devrait pas prendre plus de 30 minutes.
- *Nathan* : Pouvez-vous commencer la recherche immédiatement ? Cest très urgent.
- *Emma* : J'ai quelques petites choses à faire ce matin mais je vous communiquerai les noms dans laprès-midi.
- *Nathan* : Très bien Emma, merci. Quand vous aurez fini, pourriez vous me rappeler, comme ça je pourrai commencer à réactiver les cartes d'accès ?



- *Emma* : ok
- *Nathan* : Pourriez vous m'indiquer le temps nécessaire pour trouver linformation ?
- *Emma* : Ça ne devrait pas prendre plus de 30 minutes.
- *Nathan* : Pouvez-vous commencer la recherche immédiatement ? Cest très urgent.
- *Emma* : J'ai quelques petites choses à faire ce matin mais je vous communiquerai les noms dans laprès-midi.
- *Nathan* : Très bien Emma, merci. Quand vous aurez fini, pourriez vous me rappeler, comme ça je pourrai commencer à réactiver les cartes d'accès ?
- *Emma* : Oui, bien sûr, quel est votre numéro ?



- *Emma* : ok
- *Nathan* : Pourriez vous m'indiquer le temps nécessaire pour trouver linformation ?
- *Emma* : Ça ne devrait pas prendre plus de 30 minutes.
- *Nathan* : Pouvez-vous commencer la recherche immédiatement ? Cest très urgent.
- *Emma* : J'ai quelques petites choses à faire ce matin mais je vous communiquerai les noms dans laprès-midi.
- *Nathan* : Très bien Emma, merci. Quand vous aurez fini, pourriez vous me rappeler, comme ça je pourrai commencer à réactiver les cartes d'accès ?
- *Emma* : Oui, bien sûr, quel est votre numéro ?
- *Nathan* : Je vous donne mon numéro de téléphone mobile, comme ça vous serez sûr de me joindre : 07970 xxxxxx.



- *Emma* : ok
- *Nathan* : Pourriez vous m'indiquer le temps nécessaire pour trouver linformation ?
- *Emma* : Ça ne devrait pas prendre plus de 30 minutes.
- *Nathan* : Pouvez-vous commencer la recherche immédiatement ? Cest très urgent.
- *Emma* : J'ai quelques petites choses à faire ce matin mais je vous communiquerai les noms dans laprès-midi.
- *Nathan* : Très bien Emma, merci. Quand vous aurez fini, pourriez vous me rappeler, comme ça je pourrai commencer à réactiver les cartes d'accès ?
- *Emma* : Oui, bien sûr, quel est votre numéro ?
- *Nathan* : Je vous donne mon numéro de téléphone mobile, comme ça vous serez sûr de me joindre : 07970 xxxxxx.
- *Emma* : OK. Je vous appelle dès que j'ai fini la liste.



- *Emma* : ok
- *Nathan* : Pourriez vous m'indiquer le temps nécessaire pour trouver linformation ?
- *Emma* : Ça ne devrait pas prendre plus de 30 minutes.
- *Nathan* : Pouvez-vous commencer la recherche immédiatement ? Cest très urgent.
- *Emma* : J'ai quelques petites choses à faire ce matin mais je vous communiquerai les noms dans laprès-midi.
- *Nathan* : Très bien Emma, merci. Quand vous aurez fini, pourriez vous me rappeler, comme ça je pourrai commencer à réactiver les cartes d'accès ?
- *Emma* : Oui, bien sûr, quel est votre numéro ?
- *Nathan* : Je vous donne mon numéro de téléphone mobile, comme ça vous serez sûr de me joindre : 07970 xxxxxx.
- *Emma* : OK. Je vous appelle dès que j'ai fini la liste.
- *Nathan* : Excellent, merci. Vous me rendez un énorme service.



– *Nathan* : Pourriez vous me passer le support informatique ?



Ingénierie Sociale - Support Informatique (1/2)

- *Nathan* : Pourriez vous me passer le support informatique ?
- *Réception* : je vous les passe (longue attente ...)



Ingénierie Sociale - Support Informatique (1/2)

- *Nathan* : Pourriez vous me passer le support informatique ?
- *Réception* : je vous les passe (longue attente ...)
- *Support informatique* : Bonjour, pourrais je avoir votre numéro d'incident ou de demande ?



Ingénierie Sociale - Support Informatique (1/2)

- *Nathan* : Pourriez vous me passer le support informatique ?
- *Réception* : je vous les passe (longue attente ...)
- *Support informatique* : Bonjour, pourrais je avoir votre numéro d'incident ou de demande ?
- *Nathan* : J'aurai simplement une petite question ... cela ne vous dérange pas ?



- *Nathan* : Pourriez vous me passer le support informatique ?
- *Réception* : je vous les passe (longue attente ...)
- *Support informatique* : Bonjour, pourrais je avoir votre numéro d'incident ou de demande ?
- *Nathan* : J'aurai simplement une petite question ... cela ne vous dérange pas ?
- *Support informatique* : Quelle est elle ?



- *Nathan* : Pourriez vous me passer le support informatique ?
- *Réception* : je vous les passe (longue attente ...)
- *Support informatique* : Bonjour, pourrais je avoir votre numéro d'incident ou de demande ?
- *Nathan* : J'aurai simplement une petite question ... cela ne vous dérange pas ?
- *Support informatique* : Quelle est elle ?
- *Nathan* : Une personne de chez Reuters tente de m'envoyer une présentation et m'indique qu'il n'y arrive pas car la taille de sa pièce jointe est trop importante.



- *Nathan* : Pourriez vous me passer le support informatique ?
- *Réception* : je vous les passe (longue attente ...)
- *Support informatique* : Bonjour, pourrais je avoir votre numéro d'incident ou de demande ?
- *Nathan* : J'aurai simplement une petite question ... cela ne vous dérange pas ?
- *Support informatique* : Quelle est elle ?
- *Nathan* : Une personne de chez Reuters tente de m'envoyer une présentation et m'indique qu'il n'y arrive pas car la taille de sa pièce jointe est trop importante.
- *Support informatique* : C'est 5 Mo, Monsieur.



- *Nathan* : Pourriez vous me passer le support informatique ?
- *Réception* : je vous les passe (longue attente ...)
- *Support informatique* : Bonjour, pourrais je avoir votre numéro d'incident ou de demande ?
- *Nathan* : J'aurai simplement une petite question ... cela ne vous dérange pas ?
- *Support informatique* : Quelle est elle ?
- *Nathan* : Une personne de chez Reuters tente de m'envoyer une présentation et m'indique qu'il n'y arrive pas car la taille de sa pièce jointe est trop importante.
- *Support informatique* : C'est 5 Mo, Monsieur.
- *Nathan* : Très bien, merci. Oh, une autre chose ... Il m'a indiqué que c'était une fichier de type .exe et que parfois ces derniers étaient bloqués.



- *Support informatique* : Il ne pourra pas envoyer de fichiers .exe, l'antivirus va le bloquer. Pour quelle raison a t'il besoin d'envoyer un exécutable ?



- *Support informatique* : Il ne pourra pas envoyer de fichiers .exe, l'antivirus va le bloquer. Pour quelle raison a t'il besoin d'envoyer un exécutable ?
- *Nathan* : Je ne sais pas. Comment pourrait il me l'envoyer ? Faut il le zipper ou faire autre chose ?



- *Support informatique* : Il ne pourra pas envoyer de fichiers .exe, l'antivirus va le bloquer. Pour quelle raison a t'il besoin d'envoyer un exécutable ?
- *Nathan* : Je ne sais pas. Comment pourrait il me l'envoyer ? Faut il le zipper ou faire autre chose ?
- *Support informatique* : Les fichiers .zip sont autorisés Monsieur.



- *Support informatique* : Il ne pourra pas envoyer de fichiers .exe, l'antivirus va le bloquer. Pour quelle raison a t'il besoin d'envoyer un exécutable ?
- *Nathan* : Je ne sais pas. Comment pourrait il me l'envoyer ? Faut il le zipper ou faire autre chose ?
- *Support informatique* : Les fichiers .zip sont autorisés Monsieur.
- *Nathan* : Ok, une dernière chose. Je ne vois pas l'icône de Norton Anti-virus sur ma barre. La dernière fois, ça marchait , il y avait une petite icône.



- *Support informatique* : Il ne pourra pas envoyer de fichiers .exe, l'antivirus va le bloquer. Pour quelle raison a t'il besoin d'envoyer un exécutable ?
- *Nathan* : Je ne sais pas. Comment pourrait il me l'envoyer ? Faut il le zipper ou faire autre chose ?
- *Support informatique* : Les fichiers .zip sont autorisés Monsieur.
- *Nathan* : Ok, une dernière chose. Je ne vois pas l'icône de Norton Anti-virus sur ma barre. La dernière fois, ça marchait , il y avait une petite icône.
- *Support informatique* : Nous utilisons McAfee ici. C'est juste une icône différente, elle est bleue.



- *Support informatique* : Il ne pourra pas envoyer de fichiers .exe, l'antivirus va le bloquer. Pour quelle raison a t'il besoin d'envoyer un exécutable ?
- *Nathan* : Je ne sais pas. Comment pourrait il me l'envoyer ? Faut il le zipper ou faire autre chose ?
- *Support informatique* : Les fichiers .zip sont autorisés Monsieur.
- *Nathan* : Ok, une dernière chose. Je ne vois pas l'icône de Norton Anti-virus sur ma barre. La dernière fois, ça marchait , il y avait une petite icône.
- *Support informatique* : Nous utilisons McAfee ici. C'est juste une icône différente, elle est bleue.
- *Nathan* : Ceci explique tout. Merci, au revoir.



Conclusion

Je sais maintenant comment envoyer un fichier exécutable par courriel, je dois simplement le zipper avant et il doit faire moins de 5 Mo.



Conclusion

Je sais maintenant comment envoyer un fichier exécutable par courriel, je dois simplement le zipper avant et il doit faire moins de 5 Mo.

J'ai aussi appris qu'ils utilisaient l'antivirus McAfee.



Quelques heures plus tard, un appel de Emma des Ressources Humaines



Quelques heures plus tard, un appel de Emma des Ressources Humaines

– *Emma* : Bonjour, est ce Eric ?



Quelques heures plus tard, un appel de Emma des Ressources Humaines

- *Emma* : Bonjour, est ce Eric ?
- *Nathan* : Oui, bonjour.



Quelques heures plus tard, un appel de Emma des Ressources Humaines

- *Emma* : Bonjour, est ce Eric ?
- *Nathan* : Oui, bonjour.
- *Emma* : Je dispose de la liste des nouveaux arrivants pour vous. Souhaitez vous que je vous la faxe ?



Quelques heures plus tard, un appel de Emma des Ressources Humaines

- *Emma* : Bonjour, est ce Eric ?
- *Nathan* : Oui, bonjour.
- *Emma* : Je dispose de la liste des nouveaux arrivants pour vous. Souhaitez vous que je vous la faxe ?
- *Nathan* : Oui s'il vous plaît. Ce serait sympathique. Combien sont ils ?



Quelques heures plus tard, un appel de Emma des Ressources Humaines

- *Emma* : Bonjour, est ce Eric ?
- *Nathan* : Oui, bonjour.
- *Emma* : Je dispose de la liste des nouveaux arrivants pour vous. Souhaitez vous que je vous la faxe ?
- *Nathan* : Oui s'il vous plaît. Ce serait sympathique. Combien sont ils ?
- *Emma* : Environ 10 personnes.



Quelques heures plus tard, un appel de Emma des Ressources Humaines

- *Emma* : Bonjour, est ce Eric ?
- *Nathan* : Oui, bonjour.
- *Emma* : Je dispose de la liste des nouveaux arrivants pour vous. Souhaitez vous que je vous la faxe ?
- *Nathan* : Oui s'il vous plaît. Ce serait sympathique. Combien sont ils ?
- *Emma* : Environ 10 personnes.
- *Nathan* : Je ne suis pas sûr que le fax fonctionne correctement ici. Pourriez vous me les dire oralement ? Je pense que ça ira plus vite.



Quelques heures plus tard, un appel de Emma des Ressources Humaines

- *Emma* : Bonjour, est ce Eric ?
- *Nathan* : Oui, bonjour.
- *Emma* : Je dispose de la liste des nouveaux arrivants pour vous. Souhaitez vous que je vous la faxe ?
- *Nathan* : Oui s'il vous plaît. Ce serait sympathique. Combien sont ils ?
- *Emma* : Environ 10 personnes.
- *Nathan* : Je ne suis pas sûr que le fax fonctionne correctement ici. Pourriez vous me les dire oralement ? Je pense que ça ira plus vite.
- *Emma* : Très bien. Avez vous une crayon ?



Quelques heures plus tard, un appel de Emma des Ressources Humaines

- *Emma* : Bonjour, est ce Eric ?
- *Nathan* : Oui, bonjour.
- *Emma* : Je dispose de la liste des nouveaux arrivants pour vous. Souhaitez vous que je vous la faxe ?
- *Nathan* : Oui s'il vous plaît. Ce serait sympathique. Combien sont ils ?
- *Emma* : Environ 10 personnes.
- *Nathan* : Je ne suis pas sûr que le fax fonctionne correctement ici. Pourriez vous me les dire oralement ? Je pense que ça ira plus vite.
- *Emma* : Très bien. Avez vous une crayon ?
- *Nathan* : Oui. Je suis prêt.



Quelques heures plus tard, un appel de Emma des Ressources Humaines

- *Emma* : Bonjour, est ce Eric ?
- *Nathan* : Oui, bonjour.
- *Emma* : Je dispose de la liste des nouveaux arrivants pour vous. Souhaitez vous que je vous la faxe ?
- *Nathan* : Oui s'il vous plaît. Ce serait sympathique. Combien sont ils ?
- *Emma* : Environ 10 personnes.
- *Nathan* : Je ne suis pas sûr que le fax fonctionne correctement ici. Pourriez vous me les dire oralement ? Je pense que ça ira plus vite.
- *Emma* : Très bien. Avez vous une crayon ?
- *Nathan* : Oui. Je suis prêt.
- *Emma* : Sarah Jones, Ventes. Son manager est Roger Weaks, ...



Quelques heures plus tard, un appel de Emma des Ressources Humaines

- *Emma* : Bonjour, est ce Eric ?
- *Nathan* : Oui, bonjour.
- *Emma* : Je dispose de la liste des nouveaux arrivants pour vous. Souhaitez vous que je vous la faxe ?
- *Nathan* : Oui s'il vous plaît. Ce serait sympathique. Combien sont ils ?
- *Emma* : Environ 10 personnes.
- *Nathan* : Je ne suis pas sûr que le fax fonctionne correctement ici. Pourriez vous me les dire oralement ? Je pense que ça ira plus vite.
- *Emma* : Très bien. Avez vous une crayon ?
- *Nathan* : Oui. Je suis prêt.
- *Emma* : Sarah Jones, Ventes. Son manager est Roger Weaks, ...
- *Nathan* : Ok, merci. Vous avez été d'une aide précieuse. Au revoir.



Conclusion

Je dispose maintenant d'une liste des nouveaux arrivants dans les 2 dernières semaines. j'ai aussi les départements auxquels ils appartiennent et le nom de leur manager.



Conclusion

Je dispose maintenant d'une liste des nouveaux arrivants dans les 2 dernières semaines. j'ai aussi les départements auxquels ils appartiennent et le nom de leur manager.

Les nouveaux arrivants sont souvent plus vulnérables aux attaques de type Ingénierie Sociale que les anciens employés.



Appel au standard de la société.



Appel au standard de la société.

– *Nathan* : Bonjour, j'essaye d'envoyer un courriel à Sarah Jones mais je ne suis pas sûr de l'écriture de son adresse mail. Pourriez vous me renseigner ?



Appel au standard de la société.

– *Nathan* : Bonjour, j'essaye d'envoyer un courriel à Sarah Jones mais je ne suis pas sûr de l'écriture de son adresse mail. Pourriez vous me renseigner ?

– *Réception* : Oui, il s'agit de sarah.jones@targetcompany.com.



Appel au standard de la société.

- *Nathan* : Bonjour, j'essaye d'envoyer un courriel à Sarah Jones mais je ne suis pas sûr de l'écriture de son adresse mail. Pourriez vous me renseigner ?
- *Réception* : Oui, il s'agit de sarah.jones@targetcompany.com.
- *Nathan* : Merci.



Appel au standard de la société.

– *Nathan* : Bonjour, j'essaye d'envoyer un courriel à Sarah Jones mais je ne suis pas sûr de l'écriture de son adresse mail. Pourriez vous me renseigner ?

– *Réception* : Oui, il s'agit de sarah.jones@targetcompany.com.

– *Nathan* : Merci.

– *Nathan* : Ok, merci. Vous avez été d'une aide précieuse. Au revoir.



Quelques minutes plus tard, un email maquillé est envoyé :



Quelques minutes plus tard, un email maquillé est envoyé :

Courriel

De : itsecurity@targetcompany.com
A : sarah.jones@targetcompany.com
Sujet : Sécurité des Systèmes d'Information

Sarah,

En tant que nouvelle recrue de la compagnie, vous devez être averti de la politique de sécurité et des procédures et en particulier la politique de droit aux utilisateurs.

L'objectif de cette politique est de faire le tour des droits acceptables pour l'utilisation des ordinateurs au sein de la société. Ces règles sont en place pour protéger les employés et la compagnie ciblée. Une utilisation inappropriée vous expose à des risques tels que des attaques par virus, de compromettre les systèmes service et réseau et à des problèmes juridiques.

Cette politique est appliquée aux employés, contractuels, consultants, remplaçant et autres travailleurs pour la société, tels que tout le personnel du secteur tertiaire.

Cette politique est applicable pour tous les équipements possédés ou loués par la société.

Quelqu'un vous contactera bientôt pour parler avec vous.

Cordialement,

L'équipe de Sécurité des Systèmes d'Information



Un couple d'heures plus tard, j'appelle le standard.



Un couple d'heures plus tard, j'appelle le standard.

– *Nathan* : Bonjour, pourrais je parler à Sarah Jones, s'il vous plaît ?



Un couple d'heures plus tard, j'appelle le standard.

- *Nathan* : Bonjour, pourrais je parler à Sarah Jones, s'il vous plaît ?
- *Réception* : Je vous la passe.



Un couple d'heures plus tard, j'appelle le standard.

– *Nathan* : Bonjour, pourrais je parler à Sarah Jones, s'il vous plaît ?

– *Réception* : Je vous la passe.

– *Sarah* : Bonjour, service des ventes. Que puis-je faire pour vous ?



Un couple d'heures plus tard, j'appelle le standard.

– *Nathan* : Bonjour, pourrais je parler à Sarah Jones, s'il vous plaît ?

– *Réception* : Je vous la passe.

– *Sarah* : Bonjour, service des ventes. Que puis-je faire pour vous ?

– *Nathan* : Bonjour Sarah. Je vous appelle pour vous informer des bonnes pratiques en terme de Sécurité des Systèmes d'Information. Vous avez du recevoir un courriel de ma part.



Un couple d'heures plus tard, j'appelle le standard.

– *Nathan* : Bonjour, pourrais je parler à Sarah Jones, s'il vous plaît ?

– *Réception* : Je vous la passe.

– *Sarah* : Bonjour, service des ventes. Que puis-je faire pour vous ?

– *Nathan* : Bonjour Sarah. Je vous appelle pour vous informer des bonnes pratiques en terme de Sécurité des Systèmes d'Information. Vous avez du recevoir un courriel de ma part.

– *Sarah* : Oui en effet, j'ai reçu un courriel de votre part aujourd'hui



Un couple d'heures plus tard, j'appelle le standard.

– *Nathan* : Bonjour, pourrais je parler à Sarah Jones, s'il vous plaît ?

– *Réception* : Je vous la passe.

– *Sarah* : Bonjour, service des ventes. Que puis-je faire pour vous ?

– *Nathan* : Bonjour Sarah. Je vous appelle pour vous informer des bonnes pratiques en terme de Sécurité des Systèmes d'Information. Vous avez du recevoir un courriel de ma part.

– *Sarah* : Oui en effet, j'ai reçu un courriel de votre part aujourd'hui

– *Nathan* : OK, excellent. C'est simplement une procédure standard qui est appliquée à l'ensemble des arrivants, elle ne nécessite pas plus de 5 minutes. Comment trouvez vous l'ambiance ici ? Tout se passe bien ?



Un couple d'heures plus tard, j'appelle le standard.

– *Nathan* : Bonjour, pourrais je parler à Sarah Jones, s'il vous plaît ?

– *Réception* : Je vous la passe.

– *Sarah* : Bonjour, service des ventes. Que puis-je faire pour vous ?

– *Nathan* : Bonjour Sarah. Je vous appelle pour vous informer des bonnes pratiques en terme de Sécurité des Systèmes d'Information. Vous avez du recevoir un courriel de ma part.

– *Sarah* : Oui en effet, j'ai reçu un courriel de votre part aujourd'hui

– *Nathan* : OK, excellent. C'est simplement une procédure standard qui est appliquée à l'ensemble des arrivants, elle ne nécessite pas plus de 5 minutes. Comment trouvez vous l'ambiance ici ? Tout se passe bien ?

– *Sarah* : Oui, merci. Tout est super. On est toujours intimidé lorsque l'on prend un nouveau poste.



– *Nathan* : Oui il est toujours difficile de se rappeler de tous les noms des personnes. Est ce que Roger vous a présenté à l'ensemble du personnel ? (... *petite allusion visant à renforcer la confiance accordée par Sarah.*)



- *Nathan* : Oui il est toujours difficile de se rappeler de tous les noms des personnes. Est ce que Roger vous a présenté à l'ensemble du personnel ? (... *petite allusion visant à renforcer la confiance accordée par Sarah.*)
- *Nathan* : Emma Jones est super au pole RH si jamais vous avez besoin de quelque chose.



- *Nathan* : Oui il est toujours difficile de se rappeler de tous les noms des personnes. Est ce que Roger vous a présenté à l'ensemble du personnel ? (... *petite allusion visant à renforcer la confiance accordée par Sarah.*)
- *Nathan* : Emma Jones est super au pole RH si jamais vous avez besoin de quelque chose.
- *Sarah* : Oui, c'est Emma qui m'a fait passer mon entretien d'embauche.



- *Nathan* : Oui il est toujours difficile de se rappeler de tous les noms des personnes. Est ce que Roger vous a présenté à l'ensemble du personnel ? (... *petite allusion visant à renforcer la confiance accordée par Sarah.*)
- *Nathan* : Emma Jones est super au pole RH si jamais vous avez besoin de quelque chose.
- *Sarah* : Oui, c'est Emma qui m'a fait passer mon entretien d'embauche.
- *Nathan* : Bien, je vais vous présenter un document d'introduction à la Sécurité des Systèmes d'Information. Avez vous votre messagerie d'ouverte ? Je vous ai envoyé la présentation, ainsi nous en parlerons ensemble.



– *Sarah* : OK, je vois votre courriel



- *Sarah* : OK, je vois votre courriel
- *Nathan* : OK, double-cliquer simplement sur la pièce jointe Security Presentation.zip



- *Sarah* : OK, je vois votre courriel
- *Nathan* : OK, double-cliquer simplement sur la pièce jointe Security Presentation.zip
- *Sarah* : Il est en train de s'ouvrir avec Winzip



- *Sarah* : OK, je vois votre courriel
- *Nathan* : OK, double-cliquer simplement sur la pièce jointe Security Presentation.zip
- *Sarah* : Il est en train de s'ouvrir avec Winzip
- *Nathan* : Cliquer simplement sur Extraire et double-cliquer sur Security Presentation



- *Sarah* : OK, je vois votre courriel
- *Nathan* : OK, double-cliquer simplement sur la pièce jointe Security Presentation.zip
- *Sarah* : Il est en train de s'ouvrir avec Winzip
- *Nathan* : Cliquer simplement sur Extraire et double-cliquer sur Security Presentation
- *Sarah* : OK. ..



L'exécutable est maintenant lancé.



L'exécutable est maintenant lancé.

En fait une série de scripts et d'outils packagés ont été inclus dans le programme.



L'exécutable est maintenant lancé.

En fait une série de scripts et d'outils packagés ont été inclus dans le programme.

Parmi ces outils, un RAT, un rootkit, des keyloggers et tout ce que nous aurions besoin.



Un clic de trop . . .

Lorsque Sarah clique sur le fichier, la présentation de lance immédiatement. C'est juste une séries de slides lui indiquant qu'il ne faut pas exécuter les .exe qu'on lui envoie et d'autres bonnes pratiques. . .



Une bonne image

La présentation est marquée de tous les logos d'entreprise qui ont été convenablement copiés à partir du serveur Web publique. Ceci simplement afin d'augmenter le degré de confiance.



Une bonne image

La présentation est marquée de tous les logos d'entreprise qui ont été convenablement copiés à partir du serveur Web publique. Ceci simplement afin d'augmenter le degré de confiance.

Quelques secondes plus tard après avoir commencé la présentation, des scripts contenus dans le paquet commencent à essayer de mettre hors service McAfee ou tout autre élément de sécurité du PC qui pourrait être trouvé sur l'ordinateur de manière à le protéger.



Une bonne image

La présentation est marquée de tous les logos d'entreprise qui ont été convenablement copiés à partir du serveur Web publique. Ceci simplement afin d'augmenter le degré de confiance.

Quelques secondes plus tard après avoir commencé la présentation, des scripts contenus dans le paquet commencent à essayer de mettre hors service McAfee ou tout autre élément de sécurité du PC qui pourrait être trouvé sur l'ordinateur de manière à le protéger.

Une fois cette phase accomplie, le rootkit s'installe cachant toutes les futures actions au niveau du système d'exploitation ou toute tentative d'analyse forensic.



Une bonne image

La présentation est marquée de tous les logos d'entreprise qui ont été convenablement copiés à partir du serveur Web publique. Ceci simplement afin d'augmenter le degré de confiance.

Quelques secondes plus tard après avoir commencé la présentation, des scripts contenus dans le paquet commencent à essayer de mettre hors service McAfee ou tout autre élément de sécurité du PC qui pourrait être trouvé sur l'ordinateur de manière à le protéger.

Une fois cette phase accomplie, le rootkit s'installe cachant toutes les futures actions au niveau du système d'exploitation ou toute tentative d'analyse forensic.

Ensuite, le RAT est caché et installé.



Conclusion

Le RAT est installé de manière à démarrer en même temps que la machine et toutes ces actions sont camouflées par le rootkit.



Conclusion

Le RAT est installé de manière à démarrer en même temps que la machine et toutes ces actions sont camouflées par le rootkit.

Le RAT cherche alors la configuration d'un éventuel proxy et toute autre information utiles puis essaye de se frayer un chemin réseau vers l'Internet, prêt à obtenir des commandes de son maître.



Conclusion

Le RAT est installé de manière à démarrer en même temps que la machine et toutes ces actions sont camouflées par le rootkit.

Le RAT cherche alors la configuration d'un éventuel proxy et toute autre information utiles puis essaye de se frayer un chemin réseau vers l'Internet, prêt à obtenir des commandes de son maître.

Évidemment, tous les processus et les connexions TCP sont cachés. Ainsi même des programmes comme netstat et le gestionnaire de tâches ne verront rien.



Le RAT se connecte au serveur. Je dispose donc d'une connexion sur le PC de l'entreprise et je peux commencer à hacker le réseau !

