ATELIER SUR LA

CYBERSÉCURITÉ

PRÉSENTATION

MON PARCOURS

POURQUOI MOI ?

RETOUR SUR MON PARCOURS

LA CYBERSÉCURITÉ

C'EST QUOI :

ÇA CONCERNE QUI ?

L'ATELIER

DE QUOI ÇA PARLE ?

DEROULEMENT

SOMMAIRE

LES MALWARES

- VIRUS
- WORMS
- TROJAN
- SPYWARES
- ADWARES
- KEYLOGGERS
- RANSOMWARES
- CRYPTO MINERS
- ROOTKITS

LES MALWARES

- VIRUS
  SE PROPAGENT RAPIDEMENT D'UN ORDINATEUR À UN AUTRE ET PEUVENT CAUSER DES DOMMAGES IMPORTANTS
- WORMS
- TROJAN
- SPYWARES
- ADWARES
- KEYLOGGERS
- RANSOMWARES
- CRYPTO MINERS
- ROOTKITS

LES MALWARES

- VIRUS

SE PROPAGENT RAPIDEMENT D'UN ORDINATEUR À UN AUTRE ET PEUVENT CAUSER DES DOMMAGES IMPORTANTS

- WORMS

SE PROPAGE EN EXPLOITANT LES VULNÉRABILITÉS DES SYSTÈMES. UTILISÉS POUR VOLER DES INFORMATIONS OU PERTURBER LES RÉSEAUX

- TROJAN
- SPYWARES
- ADWARES
- KEYLOGGERS
- RANSOMWARES
- CRYPTO MINERS
- ROOTKITS

LES MALWARES

- VIRUS

SE PROPAGENT RAPIDEMENT D'UN ORDINATEUR À UN AUTRE ET PEUVENT CAUSER DES DOMMAGES IMPORTANTS

- WORMS

SE PROPAGE EN EXPLOITANT LES VULNÉRABILITÉS DES SYSTÈMES. UTILISÉS POUR VOLER DES INFORMATIONS OU PERTURBER LES RÉSEAUX

- TROJAN

SE FONT PASSER POUR DES PROGRAMMES LÉGITIMES POUR VOLER DES INFORMATIONS OU INSTALLER D'AUTRES MALWARES

- SPYWARES
- ADWARES
- KEYLOGGERS
- RANSOMWARES
- CRYPTO MINERS
- ROOTKITS

LES MALWARES

- VIRUS

SE PROPAGENT RAPIDEMENT D'UN ORDINATEUR À UN AUTRE ET PEUVENT CAUSER DES DOMMAGES IMPORTANTS

- WORMS

SE PROPAGE EN EXPLOITANT LES VULNÉRABILITÉS DES SYSTÈMES. UTILISÉS POUR VOLER DES INFORMATIONS OU PERTURBER LES RÉSEAUX

- TROJAN

SE FONT PASSER POUR DES PROGRAMMES LÉGITIMES POUR VOLER DES INFORMATIONS OU INSTALLER D'AUTRES MALWARES

- SPYWARES

SURVEILLENT L'ACTIVITÉ DE L'UTILISATEUR ET RECUEILLENT DES INFORMATIONS PERSONNELLES

- ADWARES
- KEYLOGGERS
- RANSOMWARES
- CRYPTO MINERS
- ROOTKITS

LES MALWARES

- VIRUS

SE PROPAGENT RAPIDEMENT D'UN ORDINATEUR À UN AUTRE ET PEUVENT CAUSER DES DOMMAGES IMPORTANTS

- WORMS

SE PROPAGE EN EXPLOITANT LES VULNÉRABILITÉS DES SYSTÈMES. UTILISÉS POUR VOLER DES INFORMATIONS OU PERTURBER LES RÉSEAUX

- TROJAN

SE FONT PASSER POUR DES PROGRAMMES LÉGITIMES POUR VOLER DES INFORMATIONS OU INSTALLER D'AUTRES MALWARES

- SPYWARES

SURVEILLENT L'ACTIVITÉ DE L'UTILISATEUR ET RECUEILLENT DES INFORMATIONS PERSONNELLES

- ADWARES

PRENNENT LE CONTRÔLE DE VOTRE ORDINATEUR POUR AFFICHER DES PUBLICITÉS VERS DES SITES SUSPECTS.

- KEYLOGGERS

- RANSOMWARES

- CRYPTO MINERS

- ROOTKITS

LES MALWARES

- VIRUS

SE PROPAGENT RAPIDEMENT D'UN ORDINATEUR À UN AUTRE ET PEUVENT CAUSER DES DOMMAGES IMPORTANTS

- WORMS

SE PROPAGE EN EXPLOITANT LES VULNÉRABILITÉS DES SYSTÈMES. UTILISÉS POUR VOLER DES INFORMATIONS OU PERTURBER LES RÉSEAUX

- TROJAN

SE FONT PASSER POUR DES PROGRAMMES LÉGITIMES POUR VOLER DES INFORMATIONS OU INSTALLER D'AUTRES MALWARES

- SPYWARES

SURVEILLENT L'ACTIVITÉ DE L'UTILISATEUR ET RECUEILLENT DES INFORMATIONS PERSONNELLES

- ADWARES

PRENNENT LE CONTRÔLE DE VOTRE ORDINATEUR POUR AFFICHER DES PUBLICITÉS VERS DES SITES SUSPECTS.

- KEYLOGGERS

ENREGISTRE LES FRAPPES DE CLAVIER POUR VOLER DES INFORMATIONS SENSIBLES, TELLES QUE DES MOTS DE PASSE ET DES NUMÉROS DE CARTE DE CRÉDIT

- RANSOMWARES

- CRYPTO MINERS

- ROOTKITS

LES MALWARES

- VIRUS

SE PROPAGENT RAPIDEMENT D'UN ORDINATEUR À UN AUTRE ET PEUVENT CAUSER DES DOMMAGES IMPORTANTS

- WORMS

SE PROPAGE EN EXPLOITANT LES VULNÉRABILITÉS DES SYSTÈMES. UTILISÉS POUR VOLER DES INFORMATIONS OU PERTURBER LES RÉSEAUX

- TROJAN

SE FONT PASSER POUR DES PROGRAMMES LÉGITIMES POUR VOLER DES INFORMATIONS OU INSTALLER D'AUTRES MALWARES

- SPYWARES

SURVEILLENT L'ACTIVITÉ DE L'UTILISATEUR ET RECUEILLENT DES INFORMATIONS PERSONNELLES

- ADWARES

PRENNENT LE CONTRÔLE DE VOTRE ORDINATEUR POUR AFFICHER DES PUBLICITÉS VERS DES SITES SUSPECTS.

- KEYLOGGERS

ENREGISTRE LES FRAPPES DE CLAVIER POUR VOLER DES INFORMATIONS SENSIBLES, TELLES QUE DES MOTS DE PASSE ET DES NUMÉROS DE CARTE DE CRÉDIT

- RANSOMWARES

CHIFFRE VOS FICHIERS ET EXIGE UNE RANÇON POUR LES DÉCHIFFRER

- CRYPTO MINERS

- ROOTKITS

LES MALWARES

- VIRUS

SE PROPAGENT RAPIDEMENT D'UN ORDINATEUR À UN AUTRE ET PEUVENT CAUSER DES DOMMAGES IMPORTANTS

- WORMS

SE PROPAGE EN EXPLOITANT LES VULNÉRABILITÉS DES SYSTÈMES. UTILISÉS POUR VOLER DES INFORMATIONS OU PERTURBER LES RÉSEAUX

- TROJAN

SE FONT PASSER POUR DES PROGRAMMES LÉGITIMES POUR VOLER DES INFORMATIONS OU INSTALLER D'AUTRES MALWARES

- SPYWARES

SURVEILLENT L'ACTIVITÉ DE L'UTILISATEUR ET RECUEILLENT DES INFORMATIONS PERSONNELLES

- ADWARES

PRENNENT LE CONTRÔLE DE VOTRE ORDINATEUR POUR AFFICHER DES PUBLICITÉS VERS DES SITES SUSPECTS.

- KEYLOGGERS

ENREGISTRE LES FRAPPES DE CLAVIER POUR VOLER DES INFORMATIONS SENSIBLES, TELLES QUE DES MOTS DE PASSE ET DES NUMÉROS DE CARTE DE CRÉDIT

- RANSOMWARES

CHIFFRE VOS FICHIERS ET EXIGE UNE RANÇON POUR LES DÉCHIFFRER

- CRYPTO MINERS

PIRATE L'ORDINATEUR ET L'UTILISE POUR MINER DES CRYPTOMONNAIES, UTILISATION EXCESSIVE DES RESSOURCES

- ROOTKITS

LES MALWARES

- VIRUS

SE PROPAGENT RAPIDEMENT D'UN ORDINATEUR À UN AUTRE ET PEUVENT CAUSER DES DOMMAGES IMPORTANTS

- WORMS

SE PROPAGE EN EXPLOITANT LES VULNÉRABILITÉS DES SYSTÈMES. UTILISÉS POUR VOLER DES INFORMATIONS OU PERTURBER LES RÉSEAUX

- TROJAN

SE FONT PASSER POUR DES PROGRAMMES LÉGITIMES POUR VOLER DES INFORMATIONS OU INSTALLER D'AUTRES MALWARES

- SPYWARES

SURVEILLENT L'ACTIVITÉ DE L'UTILISATEUR ET RECUEILLENT DES INFORMATIONS PERSONNELLES

- ADWARES

PRENNENT LE CONTRÔLE DE VOTRE ORDINATEUR POUR AFFICHER DES PUBLICITÉS VERS DES SITES SUSPECTS.

- KEYLOGGERS

ENREGISTRE LES FRAPPES DE CLAVIER POUR VOLER DES INFORMATIONS SENSIBLES, TELLES QUE DES MOTS DE PASSE ET DES NUMÉROS DE CARTE DE CRÉDIT

- RANSOMWARES

CHIFFRE VOS FICHIERS ET EXIGE UNE RANÇON POUR LES DÉCHIFFRER

- CRYPTO MINERS

PIRATE L'ORDINATEUR ET L'UTILISE POUR MINER DES CRYPTOMONNAIES, UTILISATION EXCESSIVE DES RESSOURCES

- ROOTKITS

CACHENT LEUR PRÉSENCE SUR UN SYSTÈME ET PERMETTENT À UN ATTAQUANT D'ACCÉDER À DISTANCE À L'ORDINATEUR

LES SOLUTIONS AUX MALWARES

- VIRUS
- WORMS
- TROJAN
- SPYWARES
- ADWARES
- KEYLOGGERS
- RANSOMWARES
- CRYPTO MINERS
- ROOTKITS

INSTALLER UN LOGICIEL ANTIVIRUS/ANTIMALWARE ET MAINTENIR SES MISES À JOUR RÉGULIÈRES.

- LOGICIELS GRATUITS : AVAST, AVG, (WINDOWS)
- LOGICIELS PAYANTS : NORTON, KASPERSKY

INSTALLER UN FIREWALL ET MAINTENIR SES MISES À JOUR RÉGULIÈRES.

- LOGICIELS GRATUITS : ZONEALARM, (WINDOWS)
- LOGICIELS PAYANTS : NORTON, MCAFEE

METTRE À JOUR RÉGULIÈREMENT LES LOGICIELS ET LES SYSTÈMES D'EXPLOITATION POUR ÉVITER LES VULNÉRABILITÉS.

NE PAS TÉLÉCHARGER DE LOGICIELS PROVENANT DE SOURCES INCONNUES ET NE PAS OUVRIR DE FICHIERS ATTACHÉS À DES E-MAILS SUSPECTS.

SAUVEGARDER RÉGULIÈREMENT LES DONNÉES POUR POUVOIR LES RÉCUPÉRER EN CAS D'ATTAQUE.

LES HACKS

- BRUTEFORCE
- DÉNI DE SERVICE (DOS ET DDOS)
- MAN-IN-THE-MIDDLE
- SPOOFING
- EVIL TWIN
- DOXING
- SWATTING

LES HACKS

- BRUTEFORCE

  TENTATIVES POUR ACCÉDER À UN SYSTÈME EN ESSAYANT DE DEVINER LES MOTS DE PASSE À PLUSIEURS REPRISES
- DÉNI DE SERVICE (DOS ET DDOS)
- MAN-IN-THE-MIDDLE
- SPOOFING
- EVIL TWIN
- DOXING
- SWATTING

LES HACKS

- BRUTEFORCE

TENTATIVES POUR ACCÉDER À UN SYSTÈME EN ESSAYANT DE DEVINER LES MOTS DE PASSE À PLUSIEURS REPRISES

- DÉNI DE SERVICE (DOS ET DDOS)

TENTATIVE POUR RENDRE UN SERVEUR OU UN RÉSEAU INDISPONIBLE EN LE SUBMERGEANT DE TRAFIC.
UTILISATION DE RESEAU ZOMBIE POUR LE DDOS

- MAN-IN-THE-MIDDLE
- SPOOFING
- EVIL TWIN
- DOXING
- SWATTING

LES HACKS

- BRUTEFORCE

TENTATIVES POUR ACCÉDER À UN SYSTÈME EN ESSAYANT DE DEVINER LES MOTS DE PASSE À PLUSIEURS REPRISES

- DÉNI DE SERVICE (DOS ET DDOS)

TENTATIVE POUR RENDRE UN SERVEUR OU UN RÉSEAU INDISPONIBLE EN LE SUBMERGEANT DE TRAFIC.
UTILISATION DE RESEAU ZOMBIE POUR LE DDOS

- MAN-IN-THE-MIDDLE

TENTATIVES POUR INTERCEPTER LES COMMUNICATIONS ENTRE DEUX PARTIES POUR VOLER DES INFORMATIONS

- SPOOFING

- EVIL TWIN

- DOXING

- SWATTING

LES HACKS

- BRUTEFORCE

TENTATIVES POUR ACCÉDER À UN SYSTÈME EN ESSAYANT DE DEVINER LES MOTS DE PASSE À PLUSIEURS REPRISES

- DÉNI DE SERVICE (DOS ET DDOS)

TENTATIVE POUR RENDRE UN SERVEUR OU UN RÉSEAU INDISPONIBLE EN LE SUBMERGEANT DE TRAFIC.
UTILISATION DE RESEAU ZOMBIE POUR LE DDOS

- MAN-IN-THE-MIDDLE

TENTATIVES POUR INTERCEPTER LES COMMUNICATIONS ENTRE DEUX PARTIES POUR VOLER DES INFORMATIONS

- SPOOFING

ATTAQUE PAR USURPATION D'IDENTITÉ DANS LAQUELLE UN PROGRAMME RÉUSSIT À S'IDENTIFIER À UN AUTRE EN FALSIFIANT DES DONNÉES (NOM DE DOMAINE, COURRIEL, ADRESSE IP)

- EVIL TWIN

- DOXING

- SWATTING

LES HACKS

- BRUTEFORCE

TENTATIVES POUR ACCÉDER À UN SYSTÈME EN ESSAYANT DE DEVINER LES MOTS DE PASSE À PLUSIEURS REPRISES

- DÉNI DE SERVICE (DOS ET DDOS)

TENTATIVE POUR RENDRE UN SERVEUR OU UN RÉSEAU INDISPONIBLE EN LE SUBMERGEANT DE TRAFIC.
UTILISATION DE RESEAU ZOMBIE POUR LE DDOS

- MAN-IN-THE-MIDDLE

TENTATIVES POUR INTERCEPTER LES COMMUNICATIONS ENTRE DEUX PARTIES POUR VOLER DES INFORMATIONS

- SPOOFING

ATTAQUE PAR USURPATION D'IDENTITÉ DANS LAQUELLE UN PROGRAMME RÉUSSIT À S'IDENTIFIER À UN AUTRE EN FALSIFIANT DES DONNÉES (NOM DE DOMAINE, COURRIEL, ADRESSE IP)

- EVIL TWIN

CRÉATION D'UN FAUX POINT D'ACCÈS WI-FI, QUI IMITE UN POINT D'ACCÈS LÉGITIME, DANS LE BUT DE VOLER DES INFORMATIONS PERSONNELLES

- DOXING

- SWATTING

LES HACKS

- BRUTEFORCE

TENTATIVES POUR ACCÉDER À UN SYSTÈME EN ESSAYANT DE DEVINER LES MOTS DE PASSE À PLUSIEURS REPRISES

- DÉNI DE SERVICE (DOS ET DDOS)

TENTATIVE POUR RENDRE UN SERVEUR OU UN RÉSEAU INDISPONIBLE EN LE SUBMERGEANT DE TRAFIC.
UTILISATION DE RESEAU ZOMBIE POUR LE DDOS

- MAN-IN-THE-MIDDLE

TENTATIVES POUR INTERCEPTER LES COMMUNICATIONS ENTRE DEUX PARTIES POUR VOLER DES INFORMATIONS

- SPOOFING

ATTAQUE PAR USURPATION D'IDENTITÉ DANS LAQUELLE UN PROGRAMME RÉUSSIT À S'IDENTIFIER À UN AUTRE EN FALSIFIANT DES DONNÉES (NOM DE DOMAINE, COURRIEL, ADRESSE IP)

- EVIL TWIN

CRÉATION D'UN FAUX POINT D'ACCÈS WI-FI, QUI IMITE UN POINT D'ACCÈS LÉGITIME, DANS LE BUT DE VOLER DES INFORMATIONS PERSONNELLES

- DOXING

ATTAQUE POUR DIVULGER DES INFORMATIONS PERSONNELLES SUR UNE PERSONNE À DES FINS MALVEILLANTES

- SWATTING

LES HACKS

- BRUTEFORCE

TENTATIVES POUR ACCÉDER À UN SYSTÈME EN ESSAYANT DE DEVINER LES MOTS DE PASSE À PLUSIEURS REPRISES

- DÉNI DE SERVICE (DOS ET DDOS)

TENTATIVE POUR RENDRE UN SERVEUR OU UN RÉSEAU INDISPONIBLE EN LE SUBMERGEANT DE TRAFIC.
UTILISATION DE RESEAU ZOMBIE POUR LE DDOS

- MAN-IN-THE-MIDDLE

TENTATIVES POUR INTERCEPTER LES COMMUNICATIONS ENTRE DEUX PARTIES POUR VOLER DES INFORMATIONS

- SPOOFING

ATTAQUE PAR USURPATION D'IDENTITÉ DANS LAQUELLE UN PROGRAMME RÉUSSIT À S'IDENTIFIER À UN AUTRE EN FALSIFIANT DES DONNÉES (NOM DE DOMAINE, COURRIEL, ADRESSE IP)

- EVIL TWIN

CRÉATION D'UN FAUX POINT D'ACCÈS WI-FI, QUI IMITE UN POINT D'ACCÈS LÉGITIME, DANS LE BUT DE VOLER DES INFORMATIONS PERSONNELLES

- DOXING

ATTAQUE POUR DIVULGER DES INFORMATIONS PERSONNELLES SUR UNE PERSONNE À DES FINS MALVEILLANTES

- SWATTING

ATTAQUE OÙ DES INDIVIDUS MALVEILLANTS FONT DES FAUSSES ALERTES AUX FORCES DE L'ORDRE, DANS LE BUT D'INCITER UNE INTERVENTION POLICIÈRE INUTILE ET DANGEREUSE CHEZ UNE PERSONNE CIBLÉE

LES SOLUTIONS AUX HACKS 1/2

- BRUTEFORCE
- DÉNI DE SERVICE (DOS ET DDOS)
- MAN-IN-THE-MIDDLE
- SPOOFING
- EVIL TWIN

UTILISER DES MOTS DE PASSE FORTS ET COMPLEXES, QUI CONTIENNENT DES LETTRES MAJUSCULES ET MINUSCULES, DES CHIFFRES ET DES SYMBOLES.

NE PAS UTILISER LE MÊME MOT DE PASSE POUR PLUSIEUR SITES

UTILISER DES OUTILS DE GESTION DES MOTS DE PASSE POUR GÉNÉRER ET STOCKER DES MOTS DE PASSE SÉCURISÉS.

VÉRIFIER L'IDENTITÉ ET LA LÉGITIMITÉ DU POINT D'ACCÈS WI-FI AVANT DE VOUS Y CONNECTER.

ÉVITER DE VOUS CONNECTER À DES RÉSEAUX WI-FI PUBLICS NON SÉCURISÉS.

UTILISER UN VPN POUR PROTÉGER VOTRE TRAFIC INTERNET LORSQUE VOUS VOUS CONNECTEZ À UN RÉSEAU WI-FI PUBLIC NON SÉCURISÉ

UTILISER UNE CONNEXION HTTPS POUR LES SITES WEB

VÉRIFIER LE CERTIFICAT SSL D'UN SITE AVANT DE SAISIR DES INFORMATIONS SENSIBLES

LES SOLUTIONS AUX HACKS 2/2

- DOXING
- SWATTING

LIMITER LA QUANTITÉ D'INFORMATIONS PERSONNELLES QUE L'ON PARTAGE EN LIGNE, Y COMPRIS SUR LES RESEAUX SOCIAUX

PROTÉGER SES INFORMATIONS PERSONNELLES EN LIGNE ET DE NE PAS PARTAGER SON ADRESSE OU D'AUTRES INFORMATIONS SENSIBLES AVEC DES PERSONNES INCONNUES.

IL EST ÉGALEMENT RECOMMANDÉ DE SIGNALER TOUT COMPORTEMENT SUSPECT À LA POLICE.

LE VPN

OUTIL QUI PERMET DE SÉCURISER ET DE PROTÉGER VOTRE CONNEXION INTERNET. EN UTILISANT UN VPN, VOUS POUVEZ CRÉER UN TUNNEL SÉCURISÉ ENTRE VOTRE ORDINATEUR OU VOTRE TÉLÉPHONE ET UN SERVEUR DISTANT, QUI PEUT SE TROUVER N'IMPORTE OÙ DANS LE MONDE.

LORSQUE VOUS VOUS CONNECTEZ À INTERNET SANS UTILISER DE VPN, VOTRE ADRESSE IP (QUI IDENTIFIE VOTRE ORDINATEUR OU VOTRE TÉLÉPHONE) EST VISIBLE PAR TOUS LES SITES QUE VOUS VISITEZ, AINSI QUE PAR VOTRE FOURNISSEUR D'ACCÈS INTERNET (FAI). CELA SIGNIFIE QUE VOS ACTIVITÉS EN LIGNE PEUVENT ÊTRE SURVEILLÉES ET QUE VOS DONNÉES PEUVENT ÊTRE COLLECTÉES, CE QUI PEUT COMPROMETTRE VOTRE VIE PRIVÉE ET VOTRE SÉCURITÉ.

AVEC UN VPN, VOUS POUVEZ MASQUER VOTRE ADRESSE IP ET LA REMPLACER PAR CELLE DU SERVEUR DISTANT QUE VOUS AVEZ CHOISI. CELA RENDRA PLUS DIFFICILE POUR LES SITES QUE VOUS VISITEZ ET VOTRE FAI DE SUIVRE VOS ACTIVITÉS EN LIGNE. DE PLUS, TOUTES LES DONNÉES QUE VOUS ENVOYEZ ET RECEVEZ EN LIGNE SERONT CRYPTÉES, CE QUI SIGNIFIE QU'ELLES SERONT PROTÉGÉES CONTRE LES PIRATES INFORMATIQUES ET LES CYBERCRIMINELS.

LOGICIELS GRATUITS : PROTON VPN, WINDSCRIBE
LOGICIELS PAYANTS : NORD VPN, CYBERGHOST VPN

LE SOCIAL ENGINEERING

- PHISHING
- SPEAR PHISING
- CATFISHING
- BLACKMAILING
- CYBER-HARCÈLEMENT

LE SOCIAL ENGINEERING

- PHISHING

TECHNIQUE UTILISÉE PAR DES FRAUDEURS POUR OBTENIR DES RENSEIGNEMENTS PERSONNELS DANS LE BUT DE PERPÉTRER UNE USURPATION D'IDENTITÉ. LA TECHNIQUE CONSISTE À FAIRE CROIRE À LA VICTIME QU'ELLE S'ADRESSE À UN TIERS DE CONFIANCE — BANQUE, ADMINISTRATION, ETC. — AFIN DE LUI SOUTIRER DES RENSEIGNEMENTS PERSONNELS

- SPEAR PHISING

- CATFISHING

- BLACKMAILING

- CYBER-HARCÈLEMENT

LE SOCIAL ENGINEERING

- PHISHING

TECHNIQUE UTILISÉE PAR DES FRAUDEURS POUR OBTENIR DES RENSEIGNEMENTS PERSONNELS DANS LE BUT DE PERPÉTRER UNE USURPATION D'IDENTITÉ. LA TECHNIQUE CONSISTE À FAIRE CROIRE À LA VICTIME QU'ELLE S'ADRESSE À UN TIERS DE CONFIANCE — BANQUE, ADMINISTRATION, ETC. — AFIN DE LUI SOUTIRER DES RENSEIGNEMENTS PERSONNELS

- SPEAR PHISING

MÊME TECHNIQUE, MAIS CIBLÉ SPECIFIQUEMENT POUR UNE PERSONNE OU UNE ENTREPRISE PRÉCISE, LE PLUS SOUVENT LE FRAUDEUR VA CHERCHER À COLLECTER UN MAXIMUM D'INFORMATION SUR SA VICTIME AVANT L'ATTAQUE AFIN DE PARAITRE PLUS CRÉDIBLE

- CATFISHING

- BLACKMAILING

- CYBER-HARCÈLEMENT

LE SOCIAL ENGINEERING

- PHISHING

TECHNIQUE UTILISÉE PAR DES FRAUDEURS POUR OBTENIR DES RENSEIGNEMENTS PERSONNELS DANS LE BUT DE PERPÉTRER UNE USURPATION D'IDENTITÉ. LA TECHNIQUE CONSISTE À FAIRE CROIRE À LA VICTIME QU'ELLE S'ADRESSE À UN TIERS DE CONFIANCE — BANQUE, ADMINISTRATION, ETC. — AFIN DE LUI SOUTIRER DES RENSEIGNEMENTS PERSONNELS

- SPEAR PHISING

MÊME TECHNIQUE, MAIS CIBLÉ SPECIFIQUEMENT POUR UNE PERSONNE OU UNE ENTREPRISE PRÉCISE, LE PLUS SOUVENT LE FRAUDEUR VA CHERCHER À COLLECTER UN MAXIMUM D'INFORMATION SUR SA VICTIME AVANT L'ATTAQUE AFIN DE PARAITRE PLUS CRÉDIBLE

- CATFISHING

ACTIVITÉ TROMPEUSE PAR LAQUELLE UNE PERSONNE SE FAIT PASSER POUR QUELQU'UN D'AUTRE, UTILISANT DE FAUSSES PHOTOS DE PROFIL, DE FAUX NOMS ET SE FAISANT SOUVENT PASSER POUR UNE PERSONNE D'UN AUTRE SEXE POUR EXTORQUER DE L'ARGENT À SES CIBLES

RÈGLE 29 : SUR INTERNET, LES HOMMES SONT DES HOMMES, LES FEMMES SONT AUSSI DES HOMMES, ET LES ENFANTS SONT DES AGENTS DU FBI SOUS COUVERTURE.

- BLACKMAILING

- CYBER-HARCÈLEMENT

LE SOCIAL ENGINEERING

- PHISHING

TECHNIQUE UTILISÉE PAR DES FRAUDEURS POUR OBTENIR DES RENSEIGNEMENTS PERSONNELS DANS LE BUT DE PERPÉTRER UNE USURPATION D'IDENTITÉ. LA TECHNIQUE CONSISTE À FAIRE CROIRE À LA VICTIME QU'ELLE S'ADRESSE À UN TIERS DE CONFIANCE — BANQUE, ADMINISTRATION, ETC. — AFIN DE LUI SOUTIRER DES RENSEIGNEMENTS PERSONNELS

- SPEAR PHISING

MÊME TECHNIQUE, MAIS CIBLÉ SPECIFIQUEMENT POUR UNE PERSONNE OU UNE ENTREPRISE PRÉCISE, LE PLUS SOUVENT LE FRAUDEUR VA CHERCHER À COLLECTER UN MAXIMUM D'INFORMATION SUR SA VICTIME AVANT L'ATTAQUE AFIN DE PARAITRE PLUS CRÉDIBLE

- CATFISHING

ACTIVITÉ TROMPEUSE PAR LAQUELLE UNE PERSONNE SE FAIT PASSER POUR QUELQU'UN D'AUTRE, UTILISANT DE FAUSSES PHOTOS DE PROFIL, DE FAUX NOMS ET SE FAISANT SOUVENT PASSER POUR UNE PERSONNE D'UN AUTRE SEXE POUR EXTORQUER DE L'ARGENT À SES CIBLES

RÈGLE 29 : SUR INTERNET, LES HOMMES SONT DES HOMMES, LES FEMMES SONT AUSSI DES HOMMES, ET LES ENFANTS SONT DES AGENTS DU FBI SOUS COUVERTURE.

- BLACKMAILING

MENACE D’ENVOYER UNE PHOTO OU UNE VIDÉO INTIME DE LA VICTIME (OU D'AUTRES INFORMATIONS SENSIBLES) À D’AUTRES PERSONNES SI LA VICTIME REFUSES DE LUI ENVOYER DE L’ARGENT OU D’AUTRES IMAGES INTIMES.

- CYBER-HARCÈLEMENT

LE SOCIAL ENGINEERING

- PHISHING

TECHNIQUE UTILISÉE PAR DES FRAUDEURS POUR OBTENIR DES RENSEIGNEMENTS PERSONNELS DANS LE BUT DE PERPÉTRER UNE USURPATION D'IDENTITÉ. LA TECHNIQUE CONSISTE À FAIRE CROIRE À LA VICTIME QU'ELLE S'ADRESSE À UN TIERS DE CONFIANCE — BANQUE, ADMINISTRATION, ETC. — AFIN DE LUI SOUTIRER DES RENSEIGNEMENTS PERSONNELS

- SPEAR PHISING

MÊME TECHNIQUE, MAIS CIBLÉ SPECIFIQUEMENT POUR UNE PERSONNE OU UNE ENTREPRISE PRÉCISE, LE PLUS SOUVENT LE FRAUDEUR VA CHERCHER À COLLECTER UN MAXIMUM D'INFORMATION SUR SA VICTIME AVANT L'ATTAQUE AFIN DE PARAITRE PLUS CRÉDIBLE

- CATFISHING

ACTIVITÉ TROMPEUSE PAR LAQUELLE UNE PERSONNE SE FAIT PASSER POUR QUELQU'UN D'AUTRE, UTILISANT DE FAUSSES PHOTOS DE PROFIL, DE FAUX NOMS ET SE FAISANT SOUVENT PASSER POUR UNE PERSONNE D'UN AUTRE SEXE POUR EXTORQUER DE L'ARGENT À SES CIBLES

RÈGLE 29 : SUR INTERNET, LES HOMMES SONT DES HOMMES, LES FEMMES SONT AUSSI DES HOMMES, ET LES ENFANTS SONT DES AGENTS DU FBI SOUS COUVERTURE.

- BLACKMAILING

MENACE D’ENVOYER UNE PHOTO OU UNE VIDÉO INTIME DE LA VICTIME (OU D'AUTRES INFORMATIONS SENSIBLES) À D’AUTRES PERSONNES SI LA VICTIME REFUSES DE LUI ENVOYER DE L’ARGENT OU D’AUTRES IMAGES INTIMES.

- CYBER-HARCÈLEMENT

PARLEZ-EN ET PORTER PLAINTE !

EXEMPLE D'ARNAQUE

SCAMS DE LOTERIE OU DE PRIX :

SCAMS DE SUPPORT TECHNIQUE :

ARNAQUES ROMANTIQUES :

ARNAQUES AUX PROCHES :

ARNAQUES DE DONS DE BIENFAISANCE :

EXEMPLE D'ARNAQUE

SCAMS DE LOTERIE OU DE PRIX : CES ARNAQUES PROMETTENT SOUVENT À LA VICTIME QU'ELLE A GAGNÉ UNE LOTERIE OU UN PRIX IMPORTANT, MAIS QU'ELLE DOIT D'ABORD PAYER DES FRAIS POUR RÉCUPÉRER SON GAIN.
(VARIANTE PRINCE NEGERIEN, HERITAGE INCONNU)

SCAMS DE SUPPORT TECHNIQUE :

ARNAQUES ROMANTIQUES :

ARNAQUES AUX PROCHES :

ARNAQUES DE DONS DE BIENFAISANCE :

EXEMPLE D'ARNAQUE

SCAMS DE LOTERIE OU DE PRIX : CES ARNAQUES PROMETTENT SOUVENT À LA VICTIME QU'ELLE A GAGNÉ UNE LOTERIE OU UN PRIX IMPORTANT, MAIS QU'ELLE DOIT D'ABORD PAYER DES FRAIS POUR RÉCUPÉRER SON GAIN.
(VARIANTE PRINCE NEGERIEN, HERITAGE INCONNU)

SCAMS DE SUPPORT TECHNIQUE : CES ARNAQUES CONSISTENT À TROMPER LA VICTIME EN LUI FAISANT CROIRE QU'IL Y A UN PROBLÈME AVEC SON ORDINATEUR OU SES LOGICIELS, PUIS À LUI PROPOSER DE L'AIDE POUR RÉSOUDRE LE PROBLÈME. LES ESCROCS DEMANDENT SOUVENT UN ACCÈS À DISTANCE À L'ORDINATEUR DE LA VICTIME, PUIS INSTALLENT DES LOGICIELS MALVEILLANTS OU DEMANDENT UN PAIEMENT POUR PRÉTENDUMENT RÉSOUDRE LE PROBLÈME.

ARNAQUES ROMANTIQUES :

ARNAQUES AUX PROCHES :

ARNAQUES DE DONS DE BIENFAISANCE :

EXEMPLE D'ARNAQUE

SCAMS DE LOTERIE OU DE PRIX : CES ARNAQUES PROMETTENT SOUVENT À LA VICTIME QU'ELLE A GAGNÉ UNE LOTERIE OU UN PRIX IMPORTANT, MAIS QU'ELLE DOIT D'ABORD PAYER DES FRAIS POUR RÉCUPÉRER SON GAIN.
(VARIANTE PRINCE NEGERIEN, HERITAGE INCONNU)

SCAMS DE SUPPORT TECHNIQUE : CES ARNAQUES CONSISTENT À TROMPER LA VICTIME EN LUI FAISANT CROIRE QU'IL Y A UN PROBLÈME AVEC SON ORDINATEUR OU SES LOGICIELS, PUIS À LUI PROPOSER DE L'AIDE POUR RÉSOUDRE LE PROBLÈME. LES ESCROCS DEMANDENT SOUVENT UN ACCÈS À DISTANCE À L'ORDINATEUR DE LA VICTIME, PUIS INSTALLENT DES LOGICIELS MALVEILLANTS OU DEMANDENT UN PAIEMENT POUR PRÉTENDUMENT RÉSOUDRE LE PROBLÈME.

ARNAQUES ROMANTIQUES : CES ARNAQUES CIBLENT SOUVENT LES PERSONNES QUI CHERCHENT L'AMOUR EN LIGNE. LES ESCROCS CRÉENT DE FAUX PROFILS SUR LES SITES DE RENCONTRE ET LES RÉSEAUX SOCIAUX, PUIS ÉTABLISSENT UNE RELATION AVEC LA VICTIME ET LUI DEMANDENT DE L'ARGENT OU DES CADEAUX.

ARNAQUES AUX PROCHES :

ARNAQUES DE DONS DE BIENFAISANCE :

EXEMPLE D'ARNAQUE

SCAMS DE LOTERIE OU DE PRIX : CES ARNAQUES PROMETTENT SOUVENT À LA VICTIME QU'ELLE A GAGNÉ UNE LOTERIE OU UN PRIX IMPORTANT, MAIS QU'ELLE DOIT D'ABORD PAYER DES FRAIS POUR RÉCUPÉRER SON GAIN.
(VARIANTE PRINCE NEGERIEN, HERITAGE INCONNU)

SCAMS DE SUPPORT TECHNIQUE : CES ARNAQUES CONSISTENT À TROMPER LA VICTIME EN LUI FAISANT CROIRE QU'IL Y A UN PROBLÈME AVEC SON ORDINATEUR OU SES LOGICIELS, PUIS À LUI PROPOSER DE L'AIDE POUR RÉSOUDRE LE PROBLÈME. LES ESCROCS DEMANDENT SOUVENT UN ACCÈS À DISTANCE À L'ORDINATEUR DE LA VICTIME, PUIS INSTALLENT DES LOGICIELS MALVEILLANTS OU DEMANDENT UN PAIEMENT POUR PRÉTENDUMENT RÉSOUDRE LE PROBLÈME.

ARNAQUES ROMANTIQUES : CES ARNAQUES CIBLENT SOUVENT LES PERSONNES QUI CHERCHENT L'AMOUR EN LIGNE. LES ESCROCS CRÉENT DE FAUX PROFILS SUR LES SITES DE RENCONTRE ET LES RÉSEAUX SOCIAUX, PUIS ÉTABLISSENT UNE RELATION AVEC LA VICTIME ET LUI DEMANDENT DE L'ARGENT OU DES CADEAUX.

ARNAQUES AUX PROCHES : LES ESCROCS RÉCOLTE DES INFORMATIONS SUR LA VICTIME PUIS LA CONTACTE EN CE FAISANT PASSER POUR UN PROCHE EN DIFFICULTÉ (ACCIDENT, BESOIN URGENT, COINCÉ A UN AUTRE ENDROIT ETC) POUR LUI DEMANDER DE L'ARGENT.

ARNAQUES DE DONS DE BIENFAISANCE :

EXEMPLE D'ARNAQUE

SCAMS DE LOTERIE OU DE PRIX : CES ARNAQUES PROMETTENT SOUVENT À LA VICTIME QU'ELLE A GAGNÉ UNE LOTERIE OU UN PRIX IMPORTANT, MAIS QU'ELLE DOIT D'ABORD PAYER DES FRAIS POUR RÉCUPÉRER SON GAIN.
(VARIANTE PRINCE NEGERIEN, HERITAGE INCONNU)

SCAMS DE SUPPORT TECHNIQUE : CES ARNAQUES CONSISTENT À TROMPER LA VICTIME EN LUI FAISANT CROIRE QU'IL Y A UN PROBLÈME AVEC SON ORDINATEUR OU SES LOGICIELS, PUIS À LUI PROPOSER DE L'AIDE POUR RÉSOUDRE LE PROBLÈME. LES ESCROCS DEMANDENT SOUVENT UN ACCÈS À DISTANCE À L'ORDINATEUR DE LA VICTIME, PUIS INSTALLENT DES LOGICIELS MALVEILLANTS OU DEMANDENT UN PAIEMENT POUR PRÉTENDUMENT RÉSOUDRE LE PROBLÈME.

ARNAQUES ROMANTIQUES : CES ARNAQUES CIBLENT SOUVENT LES PERSONNES QUI CHERCHENT L'AMOUR EN LIGNE. LES ESCROCS CRÉENT DE FAUX PROFILS SUR LES SITES DE RENCONTRE ET LES RÉSEAUX SOCIAUX, PUIS ÉTABLISSENT UNE RELATION AVEC LA VICTIME ET LUI DEMANDENT DE L'ARGENT OU DES CADEAUX.

ARNAQUES AUX PROCHES : LES ESCROCS RÉCOLTE DES INFORMATIONS SUR LA VICTIME PUIS LA CONTACTE EN CE FAISANT PASSER POUR UN PROCHE EN DIFFICULTÉ (ACCIDENT, BESOIN URGENT, COINCÉ A UN AUTRE ENDROIT ETC) POUR LUI DEMANDER DE L'ARGENT.

ARNAQUES DE DONS DE BIENFAISANCE : CES ARNAQUES EXPLOITENT LA GÉNÉROSITÉ DES GENS EN LEUR DEMANDANT DE FAIRE DES DONS À UNE CAUSE FICTIVE OU À UNE ORGANISATION CARITATIVE FICTIVE.

SOLUTIONS AU SOCIAL ENGINEERING

- PHISHING
- SPEAR PHISING
- CATFISHING
- BLACKMAILING
- CYBER-HARCÈLEMENT

NE JAMAIS DONNER D'INFORMATIONS PERSONNELLES EN RÉPONSE À DES COURRIELS OU DES MESSAGES DOUTEUX.

DEMANDER A VOTRE CORRESPONDANT SON NUMERO DE POSTE ET RAPPELER LE !

VÉRIFIER L'ADRESSE DE L'EXPÉDITEUR DU COURRIEL POUR S'ASSURER QU'ELLE EST LÉGITIME.

FAITES UNE SIMPLE RECHERCHE EN LIGNE SUR LE NOM DE L’ENTREPRISE. L’ADRESSE WEB CORRESPOND-ELLE À CELLE DU COURRIEL ?

PASSER VOTRE SOURIS SUR UN LIEN AVANT DE CLIQUER DESSUS AFIN DE VERIFIER L'ADRESSE RÉEL DU LIEN

DE MANIERE GENERAL, NE CLIQUER JAMAIS SUR UN LIEN DANS UN COURRIEL QUE VOUS NE VOUS ATTENDIEZ PAS À RECEVOIR

UTILISER UN LOGICIEL ANTIVIRUS POUR DÉTECTER LES E-MAILS DE PHISHING.

RÈGLE 29 : SUR INTERNET, LES HOMMES SONT DES HOMMES, LES FEMMES SONT AUSSI DES HOMMES, ET LES ENFANTS SONT DES AGENTS DU FBI SOUS COUVERTURE.

PARLEZ-EN ET PORTER PLAINTE !

CAS PRATIQUES

RECAP DES SOLUTIONS LOGICIELS

ANTIVIRUS/ANTIMALWARE

LOGICIELS GRATUITS : AVAST, AVG, (WINDOWS)
LOGICIELS PAYANTS : NORTON, KASPERSKY

FIREWALL

LOGICIELS GRATUITS : ZONEALARM, (WINDOWS)
LOGICIELS PAYANTS : NORTON, MCAFEE

VPN

LOGICIELS GRATUITS : PROTON VPN, WINDSCRIBE
LOGICIELS PAYANTS : NORD VPN, CYBERGHOST VPN

NAVIGATEUR

OPERA GX (BLOQUEUR DE PUB, VPN, ANTI TRACKEUR INCLUS)

RECAP DES SOLUTIONS HUMAINES

METTRE À JOUR RÉGULIÈREMENT LES LOGICIELS ET LES SYSTÈMES D'EXPLOITATION POUR ÉVITER LES VULNÉRABILITÉS.

NE PAS TÉLÉCHARGER DE LOGICIELS PROVENANT DE SOURCES INCONNUES ET NE PAS OUVRIR DE FICHIERS ATTACHÉS À DES E-MAILS SUSPECTS.

UTILISER DES MOTS DE PASSE FORTS ET COMPLEXES, QUI CONTIENNENT DES LETTRES MAJUSCULES ET MINUSCULES, DES CHIFFRES ET DES SYMBOLES.

NE PAS UTILISER LE MÊME MOT DE PASSE POUR PLUSIEUR SITES

SAUVEGARDER RÉGULIÈREMENT LES DONNÉES POUR POUVOIR LES RÉCUPÉRER EN CAS D'ATTAQUE.

NE JAMAIS DONNER D'INFORMATIONS PERSONNELLES EN RÉPONSE À DES COURRIELS OU DES MESSAGES DOUTEUX.

NE CLIQUER JAMAIS SUR UN LIEN DANS UN COURRIEL QUE VOUS NE VOUS ATTENDIEZ PAS À RECEVOIR

DE MANIERE GENERAL, SI C'EST TROP BEAU POUR ÊTRE VRAI....

QUIZZ

MERCI