



Przykłady zagrożeń

NASK





Przykłady zagrożeń

- Spam
- Phishing
- Malware
- Ransomware
- Oszustwa komputerowe
- 419, nigeryjski przekręt
- BEC, oszustwo "na dyrektora"
- Kradzież cyfrowej tożsamości

NASK



Spam

- Jakie jest źródło spamu?
 - Spam pojawia się w naszych skrzynkach pocztowych w wyniku nieuwagi.
- Jak rozpoznać spam?
 - Nasze skrzynki pocztowe otrzymują masę niechcianych wiadomości.
- Jak pozbyć się spamu?
 - Zwykle skrzynki odbiorcze mają ustawiony filtr antyspamowy.
- Jak zapobiegać spamowi?
 - Nie klikaj w linki, nie otwieraj załączników od nieznanych nadawców, nie odpowiadaj na wiadomości spamowe.

Spam

Receiving and placing orders for IT development Fratching

Ana czereta 12@adacath.com

do more

Good afternoon

We are launching the telegram channel which among other things allows developers to earn money by reselling their modules, designs and programs. And it also save your time on the purchase of ready-made solutions. For customers this is an opportunity to get better trends, vision and significantly save on development.

How it works:

Customer sent to us his task and its estimated price.

For a small commission, we publish this task in the channel.

Programmer's replies sent to us.

We send responses to the customer.

You will find more information in the channel info.

Telegram channel: <https://t.me/itreal>

Jessie vip@evg.dreamhost.com

do more

Za: rosyjski

> polski

Kryzysowi i wojownicza mentalność

S niski koszt by przywiad urzadzema okxy pod wyszyskimi zadania y e
E od Akeli \$ 25 / miesiac az do \$ 5000 / miesiac w meta-ty na keto w

MIX - 20-25k SOCKS4 / 5 - Przeglwy i portow bez

MIESZAC - 20-27k SOCKS4 / 5 Przeglwy 2-3k ma \$ 150 A miesiac

MIX - 10-15k socks4 / 5 10k plynne od 600 \$ miesiecznie

ARR ascariyos i widziny ene nam pokazac AM pokaz wyszysko Linjki taryf i ned wnetese TEST

Proxy a takze na podstawie \$ odpradkow parosowane mailing, praka z sterowania inarnego Social S / M i special Hooked zhiwaetisya dowolny rotokol twerdzemci

Budzet i inteligentne proxy dla wszelkich zadan

Paczka wiek s od **lutego 5** \$ / miesiac up to 5000 \$ / Miesiac Package F T Y P

MIX - 20-25k SOCKS4 / 5 - **Stre AMS per ts bez** e strictions R A L L protokoly - \$ am 25 H ont

MIX - 20-27k SOCKS4 / 5 2-3k strumieni \$ 150 A miesiac

MIX - 10-15 k SOCKS4 / 5 10k s strumieni 60 miesiac 0

Contact Us! bedziemy w stanie pokazac **ty cala li ne taryf** z u zapewnic test!

Each of our servers preprocessora de parling Mailin g pracujac w th sieci spolecznych Kazdy wspornik protokolem e d

pon 12 sty 11:43

☆



📄 \$ 20



Poczta Polska

Strona główna | O firmie | Biuro prasowe | Praca | Kontakt



Paczka zatrzymana w terminalu

- Wzrost brakuje płatności za fracht: 911

Nadawca: Nadawca

Opis: Nadawca

Zobacz szczegóły i historię przesyłań

Skontaktuj się

Zapłacić fracht

Dotyczy: 7-276

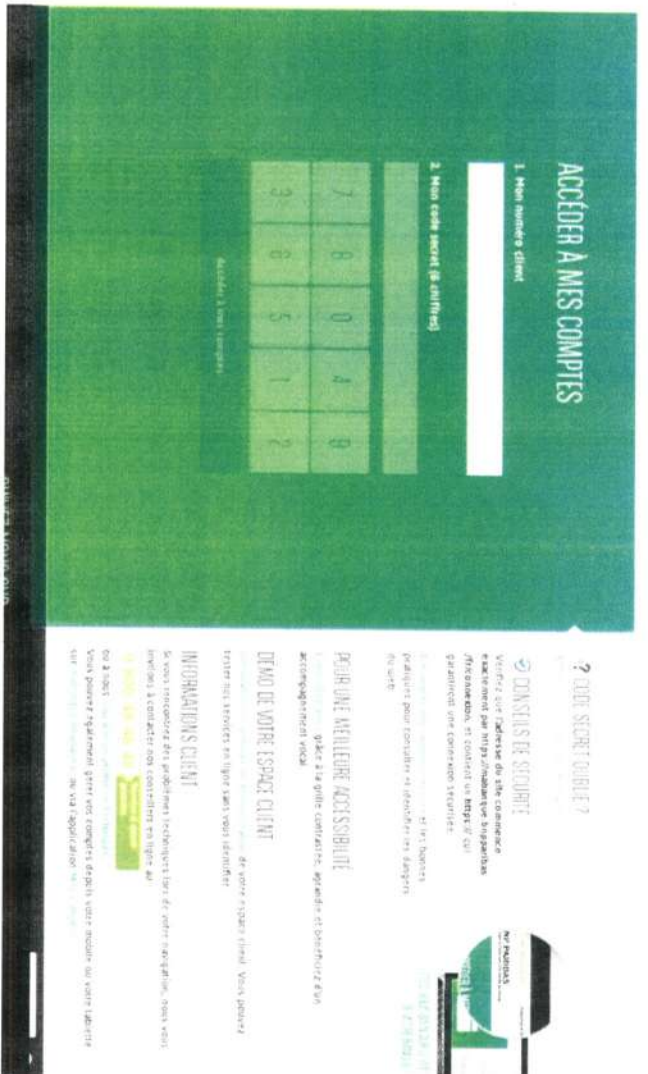
NASK

4

Phishing

- Czym jest phishing?
 - Metoda wyłudzenia danych
- Jak rozpoznać phishing?
 - Ataki phishingowe zwykle polegają na przestaniu krótkich wiadomości tekstowych, które pobudzają silne emocje.
- Metody manipulacji
 - ktoś nas okrada,
 - dzieje się krzywda twoim bliskim,
 - szantaż,
 - oskarżenie o popełnienie przestępstwa,
 - blokada środków na koncie.
- Jak postępować po zidentyfikowaniu wiadomości typu phishing?
 - Pierwsza reakcja
 - Ocena sytuacji
 - Reakcja końcowa

NASK



Anna <anna@0589230955602282.947714.love.com>
do 597348210

Hi,
Whenever you enter the building I blush.. I'm hoping you didn't notice it, I'd be very shy if you did. I'm usually quite cool with men, I don't know what happens to me when I see u :) Text me if u like..

Check out her [Profile](#) or browse her [Photo Album](#)

REPLY

Unsubscribe Me!

Report Spam

NAASK



Malware – definicje

- Czym jest Malware?
 - Infekuje urządzenia
 - Działa na szkodę użytkownika (także straty finansowe)
- Rodzaje
 - kryterium sposobu infekcji (Wirusy, robaki, trojany, inne)
 - Kryterium sposobu działania, efektu dla użytkownika (Ransomware, spyware, adware, keyloggers, rootkity)
- Źródła infekcji
 - Załącznik lub odnośnik (link) w wiadomości e-mail
 - Przejęta przez przestępców lub podstawiona, fałszywa strona
 - Podstawione reklamy na zwykłych stronach

Malware – działanie

- Jak rozpoznać malware?
 - Wykorzystywanie zasobów komputera, spowolnienie jego działania
 - Więcej spamu na pocztcie, strony startowe, których użytkownik nie ustawił w przeglądarce
 - Bardzo spektakularne działania: blokada ekranu lub systemu przy ransomware
 - **Najczęściej jednak użytkownik nic nie zauważy** – celem jest skryte działanie
- Jak zapobiegać?
 - Aktualizacje
 - Oprogramowanie antywirusowe
 - Regularne skanowanie oprogramowaniem antywirusowym
 - Kopie zapasowe danych
 - Firewall

Ransomware

- Czym jest Ransomware?
 - Jest obecnie jednym z najczęściej występujących zagrożeń w cyberprzestrzeni.
- Metody ataku i źródła infekcji
 - Złośliwe załączniki w wiadomościach e-mail zachęcających do kliknięcia,
 - Złośliwe oprogramowanie, którym komputer był już zarażony wcześniej,
 - Nieuprawniony zdalny dostęp do komputera przez osoby trzecie.
 - Atak przeprowadzony w sposób pośredni bądź bezpośredni na stację roboczą użytkownika.
- Rozpoznanie ataku
 - Najczęściej po zainfekowaniu maszyny użytkownik otrzymuje komunikat o tym, że jego dane zostały zaszyfrowane i aby odzyskać dane trzeba opłacić okup.

Ransomware

- Reagowanie podczas ataku
 - W przypadku infekcji ransomware, pozostaw komputer włączony, ale odłącz go od sieci lokalnej (Internet), żeby nie doszło do infekcji innych komputerów.
 - Zgłoś incydent do osoby odpowiedzialnej za obsługę incydentów w swoim urzędzie – helpdesku, osoby kontaktowej lub zespołu bezpieczeństwa teleinformatycznego.
- Zapobieganie atakom
 - Nie ma jednego skutecznego środka na odzyskanie zaszyfrowanych plików.
 - Twórz na bieżąco kopie zapasowych swoich danych na zewnętrznych dyskach bądź przechowuj je w chmurach.
 - Aktualizuj oprogramowanie zawierające wszelkie poprawki bezpieczeństwa.
 - Korzystaj z aktualnej wersji oprogramowania antywirusowego, nie wyłączaj funkcji heurystycznych.
 - Zwracaj uwagę na wiadomości, które otrzymujesz (email) ponieważ mogą być one częścią kampanii spamowej zawierającej zainfekowany plik. W ten sposób może dojść do infekcji poprzez otworenie zainfekowanego pliku.



Ransomware

- Nowy trend
 - Przestępcy nie oczekują okupu za zwrot danych, lecz okupu za nieupublicznienie tych danych.
- Działania przestępców
 - Przeprowadzają włamanie do sieci.
 - Wykorzystują podatności lub oprogramowanie do automatyzacji ataku.
 - Przystępują do rozpoznania sieci i systemów, kopiują dane na swój serwer, szyfrują kopie zapasowe.
 - Szyfrują system (główny atak).

Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payments>. Best time to check: 9:00am - 11:00am



Send \$300 worth of bitcoin to this address:

1Zt9YDPgwuez9Nymgw519p7AA8jsj6SMw

Copy

[Check Payment](#)

[Decrypt](#)

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

05:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

Oszustwo komputerowe

- Kodeks karny określa przestępstwa komputerowe oraz powiązane z nim artykuły dot. ochrony informacji (niejawnych, danych osobowy etc.).
- W kodeksie karnym przestępstwo komputerowe (art. 287 k.k.). Czyn zabroniony polega na wpływie na komputerowe zapisy informacji.
- Sprawcą oszustwa komputerowego może być każdy. Jest to powszechne przestępstwo. Przyjęto, że do popełnienia przestępstwa wymagany jest zamiar bezpośredni. Oznacza to, że sprawca popełniający czyn zabroniony w zamiarze bezpośrednim ma świadomość i wolę realizacji tego czynu.

Oszustwo komputerowe

Uwzględniając charakterystykę metod wykorzystywanych przez przestępców oraz zorganizowane grupy przestępcze, można wskazać następujące konsekwencje działań cyberprzestępców:

- Kradzież informacji
- Szyfrowanie informacji celem żądania okupu za odszyfrowanie danych
- Ujawnienie tajnych oraz prywatnych informacji (w tym danych osobowych)
- Niszczenie danych o strategicznym znaczeniu
- Straty finansowe
- Paraliż w sektorze prywatnym oraz w instytucjach państwowych
- Niedostępność usług internetowych

419, Nigeryjski przekręt

- Czym jest 419?
 - Oszustwo 419 wzięło nazwę od numeru artykułu z nigeryjskiego kodeksu karnego.
 - Jest znane od XVI wieku. Wówczas nazywało się Listem Hiszpańskiego Więźnia.
- Metoda ataku
 - Oszustwo polega na wciągnięciu ofiary w grę psychologiczną poprzez wysyłanie e-maili. Przestępcy wykorzystują różne metody, żeby wyłudzić pieniądze. Najczęściej spotykane to podawanie się za:
 - uchodźcę politycznego,
 - dziedzica fortuny utraconej w trakcie przewrotu politycznego,
 - syna obalonego przywódcy jednego z państw afrykańskich.
- Zapobieganie
 - Nie odpisuj na podejrzane wiadomości i zaznaczaj je jako spam.
 - Nie przesyłaj danych osobowych, numerów kont bankowych, informacji dotyczących polis ubezpieczeniowych.
 - Podchodź z dystansem do historii opisywanych w mediach społecznościowych, portalach internetowych.
 - Nie daj się skusić dużymi sumami pieniędzy. Propozycja ogromnej kwoty za pomoc uchodźcy politycznemu może być kłamstwem.

419, Nigeryjski przekręt



FDJ <info@cox.net>
do

pon., 20 kwi, 12:20



Ta wiadomość może być niebezpieczna

Podobne wiadomości posłużyły już w przeszłości do kradzieży danych osobowych. Nie klikaj żadnych linków, nie pobieraj załączników ani nie odpowiadaj z użyciem swoich danych osobowych.

Wygląda bezpiecznie

Attn: You have a charity donation of \$ 1,500,000.00 from Mrs. Julie Leach, a power-ball jackpot lottery winner of \$ 310 Million. For claim Reply to: julieleach014@yahoo.com

NASK

17
...

BEC, oszustwo "na dyrektora"

- Czym jest BEC?
 - Atak BEC, czyli Business Email Compromise wykorzystuje phishing ukierunkowany na instytucje, przedsiębiorstwa i organizacje.
- Metody manipulacji
 - Metoda oparta jest na socjotechnice stosowanej wobec pracownika firmy.
 - Atakujący wywiera wpływ poprzez nakłonienie do szybkiego wykonania określonego zadania nałożonego przez „kierownictwo wyższego szczebla”.
- Sposób ataku
 - Przestępcy prowadzą skanowanie sieci, aby odnaleźć słabe punkty w systemie.
 - Prowadza podstęp, celem uzyskania dostępu do informacji takich jak korespondencja wewnątrz organizacji, zawartość baz danych i treść innych ważnych dokumentów.
- Znaki ostrzegawcze, na które powinniśmy zwrócić uwagę w czasie takiego ataku:
 - Bezpośredni kontakt kierownictwa z pracownikiem za pośrednictwem poczty mailowej lub połączenia telefonicznego, a nie w interakcji twarzą w twarz,
 - Prośba o zachowanie pełnej poufności,

BEC, oszustwo "na dyrektora" - zapobieganie

Jako organizacja:

- Trzeba być świadomym ryzyka i informować pracowników o możliwości wystąpienia tego typu zagrożeń;
- Należy zwrócić uwagę pracowników do ostrożnego podejścia podczas dokonywanych płatności, szczególnie na wielkie sumy; Należy dbać o aktualizacje zabezpieczeń technicznych;
- W przypadku oszustwa należy kontaktować się z policją.

Jako pracownik:

- O każdym podejrzanym mailu bądź telefonie informuj swój dział IT/bezpieczeństwa.
- Nie przekazuj informacji związanych z Twoją organizacją (procedury, hierarchia organizacji).
- W serwisach społecznościowych zastosuj zasadę ograniczonego zaufania i ogranicz informacje dotyczące Twojej organizacji.
- Nigdy nie otwieraj podejrzanych linków, załączników. Otwieraj te, których się spodziewasz lub potwierdź u nadawcy (jeśli to znajomy, współpracownik), że to on wysłał tego maila. Zachowaj szczególną ostrożność podczas korzystania z osobistej skrzynki pocztowej korzystając ze sprzętu firmowego.
- Ściśle stosuj się do wewnętrznych procedur dotyczących płatności i zamówień.

BEC, oszustwo "na dyrektora"

Od Jacek [REDACTED] <officemail018@gmail.com> ☆

Temat **Pilne**

Do Skarbnik@ [REDACTED] ☆

Musimy dokonac pilnej platnosci w wysokosci 95 455,25 PLN. Czy mozemy dokonac tej platnosci dzisiaj?

Pozdrowienia
Jacek [REDACTED]

Od Adam [REDACTED] <emailsoffice@naver.com> ☆

Temat **Zapłata**

Do [REDACTED]@powiat [REDACTED] ☆

Czy możemy dziś zapłacić 36 tysięcy euro?

pozdrowienia
Adam [REDACTED]

From: [mailto:officemail045@gmail.com]
Sent: Friday, July 5, 2019 8:27 AM
To: [REDACTED]
Subject: Pilne

Musimy dokonac pilnej platnosci w wysokosci 75 455,25 PLN. Czy mozemy dokonac tej platnosci dzisiaj?

Pozdrowienia

Wysłane z mojego urządzenia mobilnego.

NASK



Kradzież cyfrowej tożsamości

Po co przestępcom twoje dane osobowe?

- Dokonają kradzieży pieniędzy z twojego konta bankowego
- Zaciągną pożyczkę na twoje dane
- Wykorzystają twoje dane, aby zrobić z ciebie „stupa”
- Będą szantażować ciebie wykradzionymi danymi

Kradzież cyfrowej tożsamości

- Gdy zakładasz profil należy rozważyć czy konieczne jest, aby profil zawierał imię i nazwisko użytkownika.
- Używaj silnego hasła (najlepiej składające się z losowych znaków – np. manager hasel) i inne niż wykorzystywane w pozostałych serwisach.
- Skonfiguruj ustawienia prywatności konta.
- Pamiętaj, że informacją jest:
 - tekst,
 - zdjęcie lub film,
 - charakterystyczne obiekty pozwalające na identyfikację Twojego miejsca przebywania lub Twoich bliskich,
 - polubione miejsca (jak również „meldowania”) lub grupy, do których należysz
- Pamiętaj, że korzystając z serwisów społecznościowych łatwo można (również nieintencjonalnie) zdradzić poufne i wrażliwe dane osób trzecich, pracodawcy, kontrahenta
- Nie należy korzystać z prywatnych profili w celach zawodowych oraz przechowywać lub przesyłać dokumentacji służbowej za pomocą zewnętrznych nieautoryzowanych serwisów
- Skasuj swój profil w serwisie, z którego nie będziesz więcej korzystać
- Jeśli padłeś ofiarą przestępstwa internetowego nie kasuj żadnych danych, sporządź kopię całej korespondencji



Kradzież cyfrowej tożsamości

Pamiętaj, Twoje dane osobowe są cenne dla przestępców.

Ochrona przed oszustwami oznacza także ich bezpieczeństwo.

NASK

Kradzież cyfrowej tożsamości



Polski English (US) Português Deutsch Français (France) Italiano 日本語 日本語 (Español) Español (España) Tiếng Việt Português (Brasil) ...

Receptacja Zaloguj się Messenger Facebook Lite Facebook Mobile Skądś znajomy Ci Wzrost Miejsca Gdzie Lokalizacja Gracze Grupy O Facebooku
Usługa reklam Usługa strony Tworzy aplikacje Polska Prywatność Polityka Prywatności Opcje wysłania reklam Reklamuj Pomoc

Facebook © 2019

NASK

mgr Izabela Słowińska
im. Tomaszowski