
OD PĘDZĄCYCH TIRÓW DOM PANA ANDRZEJA (54 l.) SIĘ TRZĘSIE
TP-LINK
300Mbps
Wireless N
Router
GODZ. 2.00
GDY INNI SŁODKO ŚPIĄ,
ANDRZEJ BEDNAREK
TRZYMA KREDENS
Nie śpię
bo trzymam
ROUTER

Nie śpię,
bo łatam modemy !

Przemysław Dęba
Przemyslaw.Deba@orange.com

Piotr Konieczny
routery@niebezpiecznik.pl

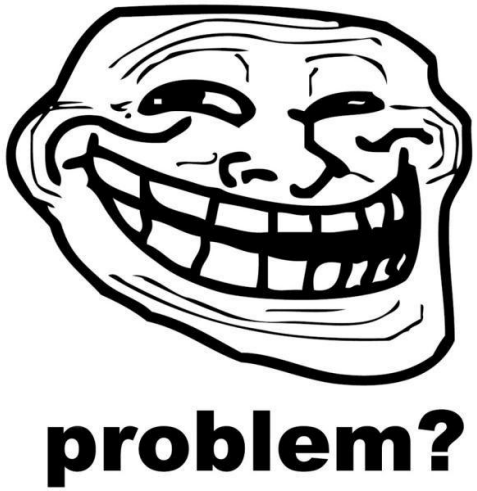
Jest dziura .

- Abdelli Nassereddine odkrywa podatność w routerze TD-W8951ND, który pracuje pod kontrolą **ZynOS** firmy **ZYXEL**
  - Z ZynOS, oprócz **TP-Link** korzystają też: **Pentagram, DLink, EDIMAX, ZTE**

- Błąd polega na możliwości wygenerowania i pobrania backupu ustawień routera przez dowolnego internautę (backup zawiera hasło administratora)
  - http://IP_ROUTERA/rpFWUpload.html - generuj backup
  - http://IP_ROUTERA/rom-0 - pobierz backup
  - http://198.61.167.113/zynos/decoded.php - zdekoduj hasło

niebezpiecznik.pl

Jakie ryzyko?



- Nieuprawniony dostęp do routera to **podsłuch internauty** lub **ataki MITM**
  - np. **PHARMING**, czyli podmiana serwerów DNS.
- W Polsce jest **ponad 1 000 000 podatnych na atak urządzeń** (wg Shodana)
- ...a niektórzy zarzucają nam, że “siejemy panikę”...
  - już następnego dnia na Karachanie pojawia się trollowanie, zachętna do podmiany SSID routerów podatnych na atak na “wiadome treści”.

niebezpiecznik.pl

STYCZEŃ

23

Na szczęście . . .

Wasze modemy są bezpieczne. Po uzyskaniu informacji o przeszło milionie modemów w polskiej sieci, nad którymi cyber-przestępcy mogą przejąć kontrolę, sprawdziliśmy, jak ma się sytuacja z urządzeniami dostępnymi kiedykolwiek w naszej sieci sprzedaży. Domyślnie mają one zablokowaną funkcję zdalnego dostępu do ustawień - analiza, wykonana przez moich kolegów z Bezpieczeństwa Systemów Teleinformatycznych Orange Polska wykazała, że jedynie 9 spośród nich jest podatnych na opisywany atak. To zaledwie 0,015 proc. wszystkich urządzeń!

- Artykuł na orange.blog.pl
- Uruchomienie narzędzia do samodzielnego testu 

Z zewnętrznej sieci na szczęście bezpiecznie, a więc skaner Orange specjalnie pisze swoim klientom, że jest zagrożenie żeby wyciągnąć kasę jakby nowy sprzęt chcieli czy coś.

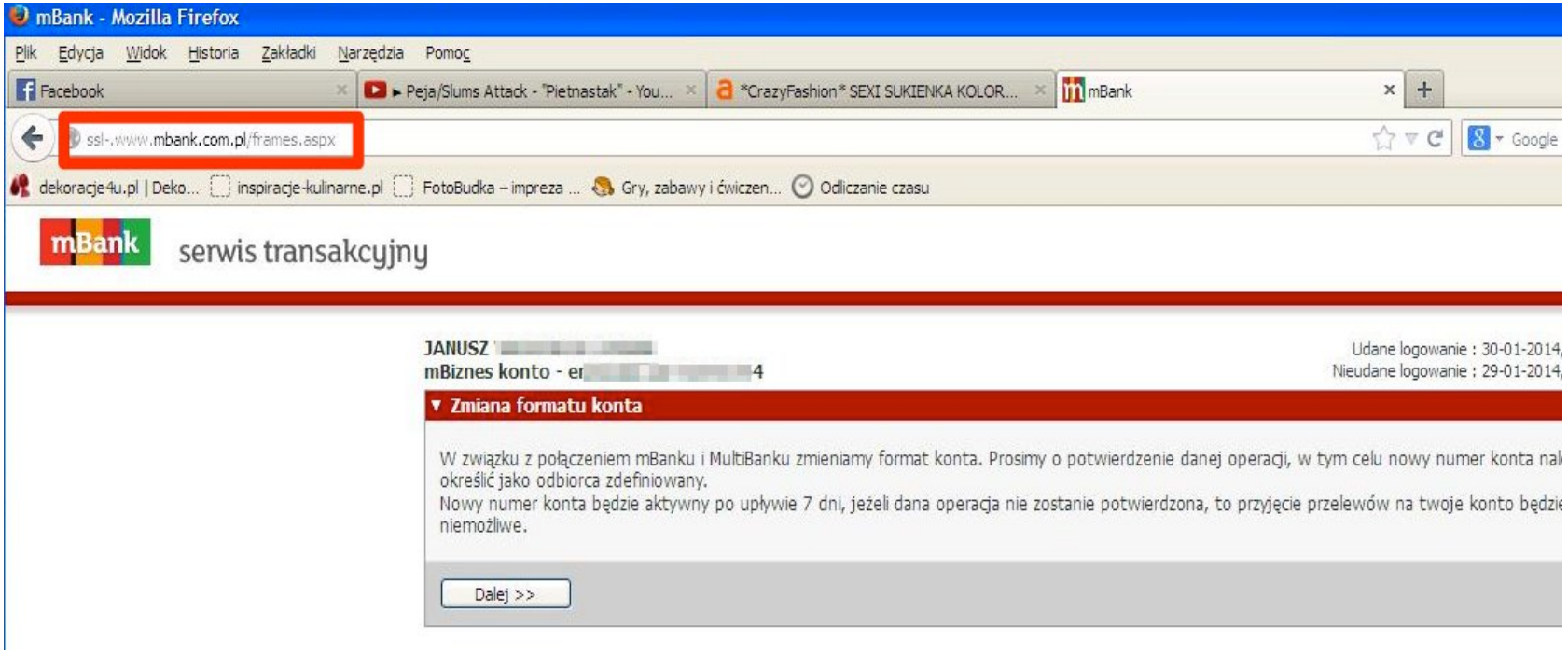
Potwierdzam. Te mialem wpisane DNS 5.45.75.36 – 5.45.75.11
Zmieniem ustawienia w TP-Linku na te ktore podal KOLA i na stronie Orange jest ju wszystko OK.

LUTY

2

Mija 15 dni ...

“Wczoraj jeden z naszych czytelników opisał nam, jak z powodu powyższej dziury w routerze, z jego konta w mBanku zniknęło **16 000** PLN.”



niebezpiecznik.pl

LUTY

2

Nie można połączyć się z prawdziwą witryną ssl-.online.mbank.pl

Coś zakłóca bezpieczne połączenie z ssl-.online.mbank.pl.

Spróbuj ponownie załadować tę stronę za kilka minut lub po przełączeniu do nowej sieci. Jeśli ostatnio łączyłeś się z nową siecią Wi-Fi, zakończ logowanie przed ponownym ładowaniem.

Jeśli wejdziesz teraz na ssl-.online.mbank.pl, może to spowodować udostępnienie prywatnych informacji intruzowi. Aby chronić Twoją prywatność, Chrome nie załaduje tej strony, dopóki nie nawiąże bezpiecznego połączenia z prawdziwą witryną ssl-.online.mbank.pl.

Odśwież | Mniej

Co to oznacza?

Witryna ssl-.online.mbank.pl zwykle chroni informacje przez ich szyfrowanie (SSL). Tym razem próba połączenia Chrome z witryną ssl-.online.mbank.pl spowodowała zwrócenie z witryny ssl-.online.mbank.pl nietypowych i niepoprawnych danych uwierzytelniających. Atakujący podszywa się pod witrynę ssl-.online.mbank.pl lub ekran logowania Wi-Fi spowodował przerwanie połączenia. Twoje dane są bezpieczne, ponieważ przeglądarka Chrome zatrzymała połączenie przed ich wymianą.

Błędy sieciowe i ataki zwykle trwają chwilę, więc strona prawdopodobnie będzie działać później. Możesz też spróbować przełączyć się do innej sieci.

Szczegóły techniczne

Witryna ssl-.online.mbank.pl żąda blokowania przez Chrome certyfikatów z błędami, a certyfikat odebrany przez Chrome podczas tej próby połączenia zawiera błąd.
Typ błędu: HSTS failure

niebezpiecznik.pl

LUTY

4

Kto naciśnie?

*Jeden z naszych klientów, duża instytucja finansowa, w godzinach wieczornych prosi dyżurnego Orange CERT o **blokadę** ruchu do fałszywych DNS ...*

@Tom: najpierw zdaj sobie sprawę z tego jaki odsetek ludzi rzeczywiście wie od czego jest kłódka w pasku przeglądarki i co się liczy w bezpiecznej sesji podczas logowania a potem pisz takie bzdury. 9/10 osób z mojego otoczenia nie ma w ogóle o tym zielonego pojęcia.

a ja sptraciloem przez 16 k zl ku****wa mac.... przez router airwire.. brak zabezpieczen . podstawili mi strone w mbnaku inna.. a ja z rutyny wisalem haslo. :(walka z bankiem bezskuteczna... prokuratura – idzie innym tropem

a może by tak zasugerować to CERT polska i żeby dostali zgodę od prokuratury itd ?

orange™

Alea iacta est .

Dziś wielu Polaków posiadających internet od Orange (TP SA) miało "problem z dostępem do internetu". Tę odważną decyzję o nałożeniu blokady podjął dział bezpieczeństwa Orange. I bardzo dobrze. Ci klienci, którzy zostali "odcięci" są bowiem zhackowani — ktoś, włamał im się na routery Wi-Fi za pomocą opisywanej przez nas ostatnio **poważnej dziury** i podmienił DNS-y na takie, które przekierowują na fałszywe strony banków. Kilka dni temu opisaliśmy **historię jednej z ofiar, która w ten sposób straciła 16 000 PLN**. Ale potencjalnych ofiar w Polsce może być aż milion! i zwłaszcza ci, którzy nie mają internetu od Orange są obecnie narażeni na ataki.

Współczuję konsultantom online. No i gratulacje dla Oranguata, cokolwiek by nie mówic o tej korporacji, to krok naprawdę w dobrą stronę. Ciekawe tylko ile w tym polityki, a ile troski o użytkownikow.

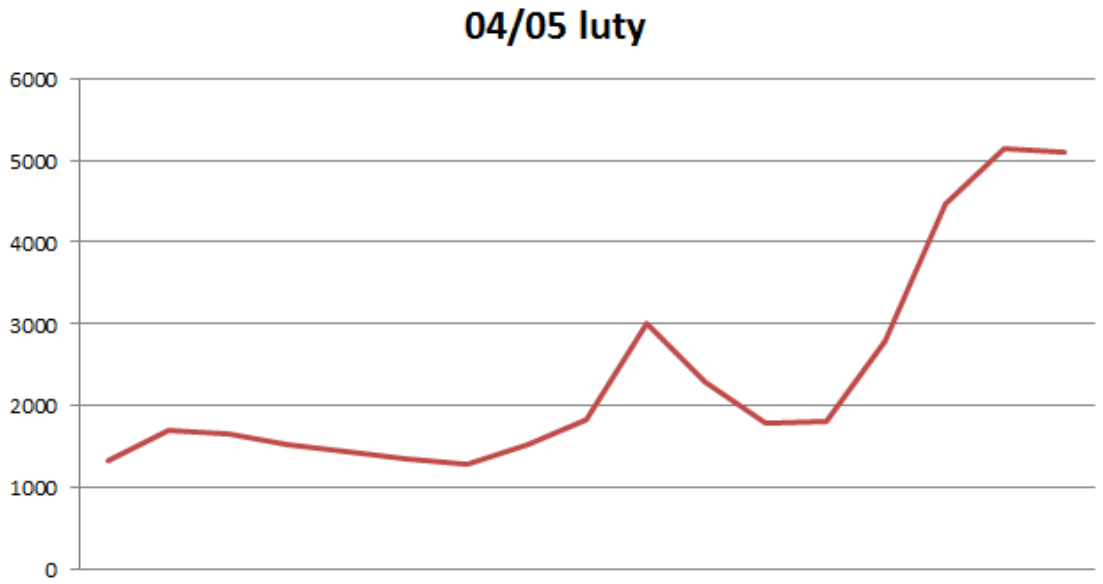
W kazdym razie rozwiazania maja swoje plusy i minusy. Zrobili jak zrobili. Bo albo nie wpadli na nic lepszego, albo wymagalo za duzo pracy/bylo za drogie/blablabla...
Dobrze zrobili, ze przynajmniej klientow zabezpieczaja ;)

Rozterki Niebezpiecznika

- Napływają coraz to **nowe zgłoszenia** od czytelników co do:
  - Podatnych na ataki modeli routerów
  - Adresów IP fałszywych DNS
  - autorskich "metod" łatania
  - *modus operandi atakujących* z honeypotów
- Niektórzy z czytelników prowadzą własne "skany" sieci i **"leczą" zarażone routery**
  - mamy dylemat jak z nimi rozmawiać...
- Inni operatorzy pytają o rady lub podsyłają wprost informacje prasowe o włączeniu własnych filtrów "takich jak Orange"

niebezpiecznik.pl

Na ratunek infolinii



- Uruchamiamy **sinkholing** na własne DNS, sieć się gotuje ..
- Powstaje **captive portal** z instrukcją rekonfiguracji routerów
- Umieszczamy na portalu **narzędzie do samonaprawy**
- Działa **honeypot** do wyłapywania nowych DNS
- Skaner na bieżąco podaje liczbę podatnych i zainfekowanych

orange™

LUTY

20

Jest motywacja!

ZWIĄZEK BANKÓW POLSKICH

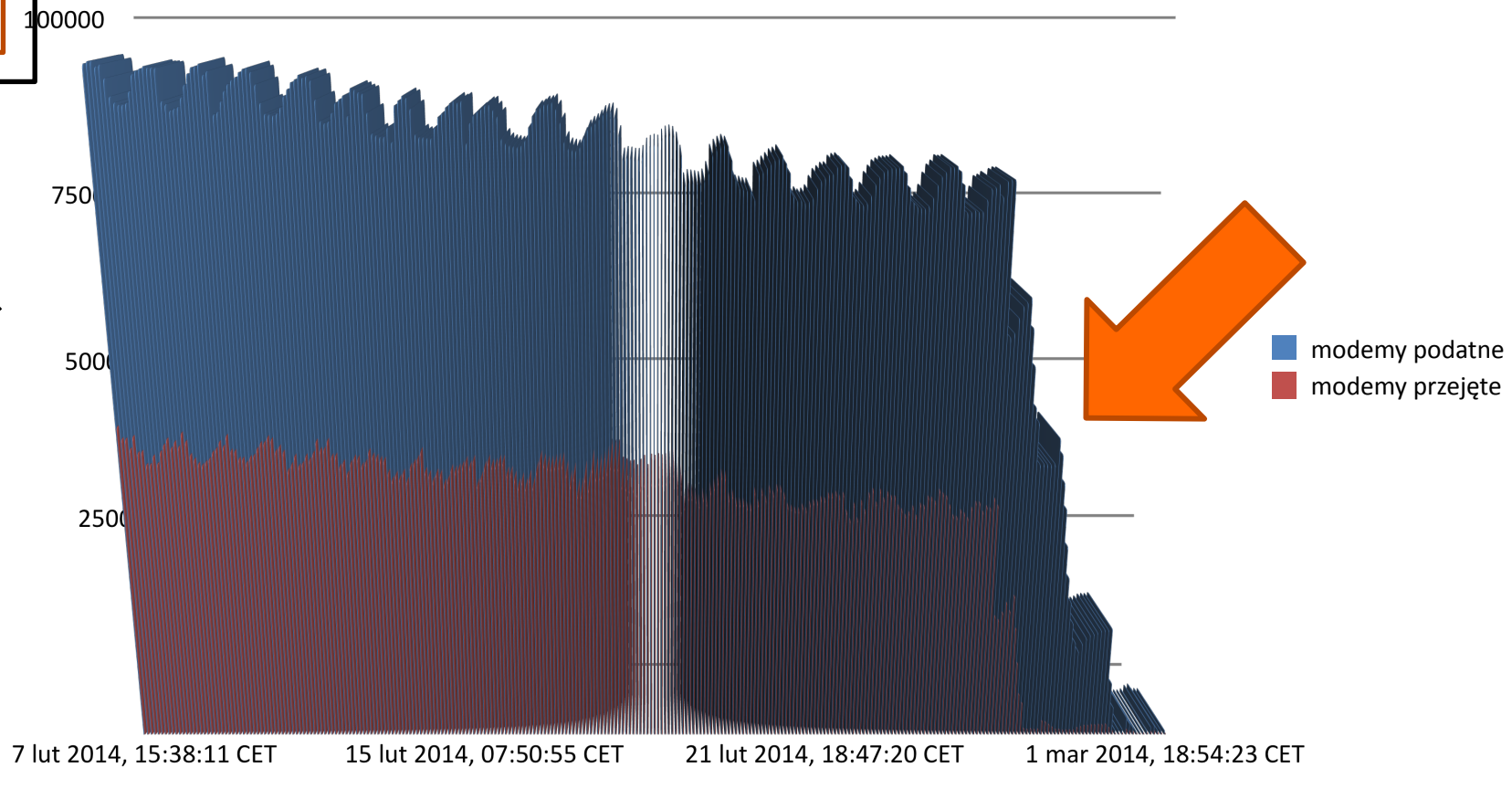
Dzięki szybkiej i skutecznej reakcji z Państwa strony został odparty atak hakerów, który był zagrożeniem dla nie tylko dla klientów korzystających z bankowości elektronicznej ale również dla użytkowników korzystających z e-usług. Dzięki temu ochroniona została ich tożsamość elektroniczna, która w przypadku nie podjęcia tej akcji mogłaby być wykorzystana do popełniania przestępstw.

orange™

LUTY

27

Cuda się zdarzają



Koszty 182 tys. zł

Poz.	Nazwa botnetu	Liczba adresów IP	Udział procentowy
1	Conficker	45521	26,79%
2	Sality	24080	14,17%
3	ZeroAccess	19025	11,20%

Neostrada 1,9 mln
BSA 0,3 mln

orange™

Odsiecz nadchodzi

W wyniku naszego zawiadomienia z dnia 6 lutego organa ścigania zapraszają nas do współpracy ...

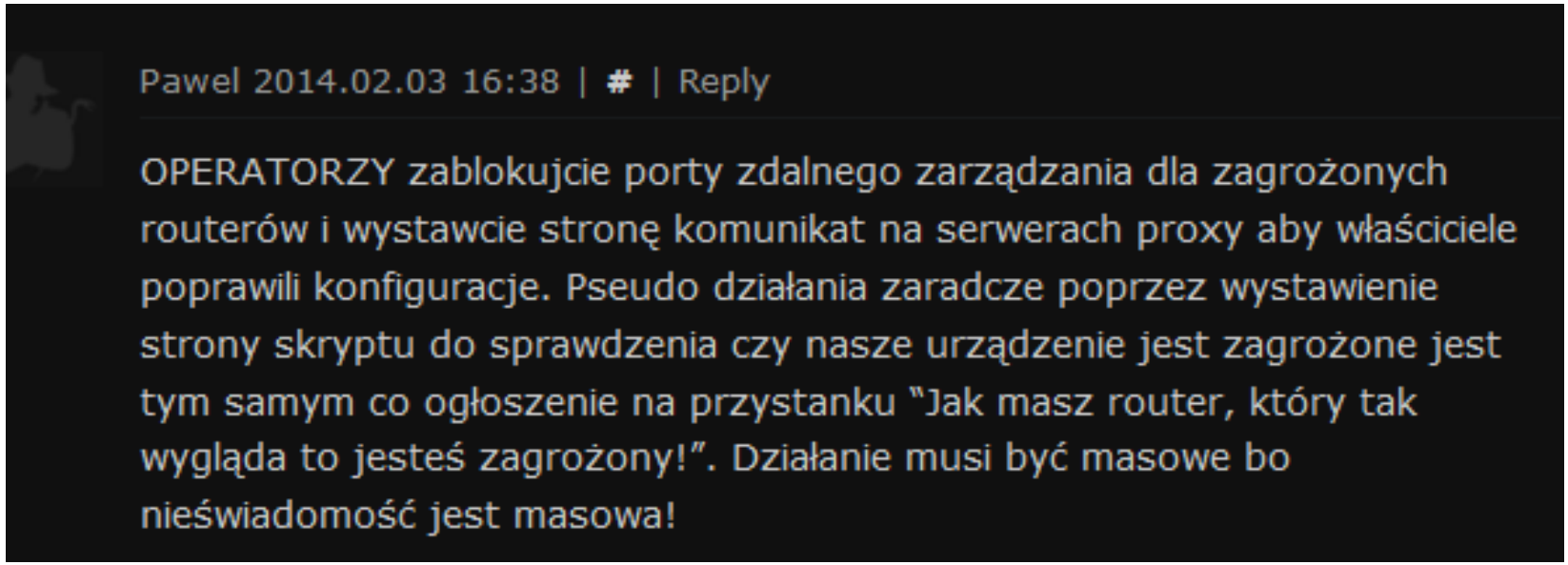
Wołanie na puszczy

- Użytkownicy internetu?!
- Operatorzy?!
- Banki?!
- Instytucje państwowe?!
- Security community?!
- Dostawcy sprzętu?!

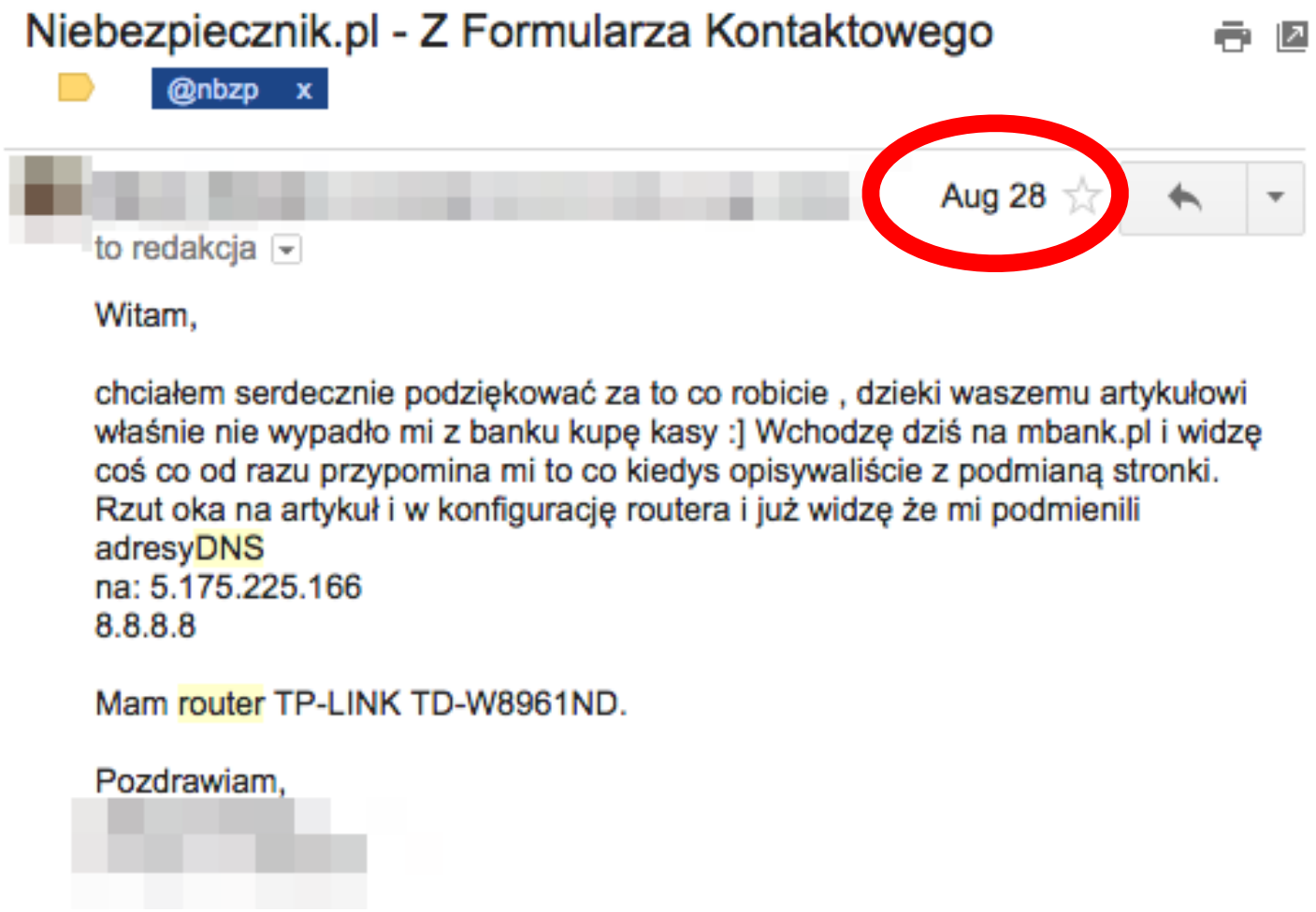
Jak Niebezpiecznik może wspierać obsługę incydentu?

- Publikowane u nas informacje mogą być **sygnałem wczesnego ostrzegania**, że coś jest (będzie) problemem...
- **Szybko zbieramy "intel"** z racji szerokiego i świadomego technicznie community (tu: *nowe IP DNS-ów, nowe modele podatnych urządzeń, sposoby obejść, dane z prywatnych honeypotów*)
- O ile są poprawne stosunki z vendorem (jak z Orange), możemy **sprawniej i wydajniej prezentować komunikaty techniczne**, które standardową ścieżką (np. publikacją na blogu Orange) nie dotarłyby TAK SZYBKO DO TAK WIELU odbiorców.

Orange odpowiada



Było warto. . .



Niebezpiecznik.pl - Z Formularza Kontaktowego

@nbzp x

[redacted] Aug 28

to redakcja

Witam,

chciałem serdecznie podziękować za to co robicie , dzieki waszemu artykułowi właśnie nie wypadło mi z banku kupę kasy :] Wchodzę dziś na mbank.pl i widzę coś co od razu przypomina mi to co kiedys opisywaliście z podmianą stronki. Rzut oka na artykuł i w konfigurację routera i już widzę że mi podmienili adresyDNS
na: 5.175.225.166
8.8.8.8

Mam router TP-LINK TD-W8961ND.

Pozdrawiam,
[redacted]

niebezpiecznik.pl

Dziękujemy ☺

Przemysław Dęba
Przemyslaw.Deba@orange.com

Piotr Konieczny
routery@niebezpiecznik.pl