Zaufana Trzecia Strona

Wybuch ropociągu w roku 2008 był dziełem hakerów a nie zwyłym zamachem

Adam dodał 10 grudnia 2014 o 23:04 w kategorii Włamania z tagami: atak • infrastruktura krytyczna • Rosja • rurociąg • Turcja

Kiedy w sierpniu 2008 wybuchł ropociąg łączący Azerbejdżan z Morzem Śródziemnym, do zamachu przyznali się Kurdowie. Dopiero dzisiaj dowiadujemy się, że wybuch był jednym z pierwszych cybernetycznych ataków na infrastrukturę krytyczną.

Kurdowie w roku 2008 nie dysponowali wystarczającą wiedzą i doświadczeniem, by przeprowadzić atak informatyczny. Kto zatem stał za wydarzeniami z sierpniowego wieczoru? Według najnowszej publikacji Bloomberga najwięcej na ataku mogli zyskać Rosjanie.

Tajemniczy wybuch

Kiedy 6 sierpnia o 11 wieczorem nagle zapalił się i wybuchł fragment ropociągu prowadzącego z Morza Kaspijskiego nad Morze Śródziemne, zawiodły wszystkie mechanizmy bezpieczeństwa. Czujniki ciśnienia nie wykazały żadnych anomalii a obsługa ropociągu o wybuchu dowiedziała się dopiero po 40 minutach od strażnika, który zauważył ogień. Nie pomogły także awaryjne systemy monitoringu, oparte o łączność satelitarną a 60 godzin zapisu z kluczowych kamer bezpieczeństwa zniknęło bezpowrotnie. Turecki rząd twierdził, że katastrofa była wynikiem awarii, ale zbyt wiele czynników wskazuje na inny scenariusz wydarzeń.

Przebieg rurociągu i miejsce ataku (źródło: Bloomberg)

Wybuch miał taką siłę, że falę uderzeniową odczuwano ok. 700 metrów od jego miejsca. Eksplozja spowodowała wyciek ok. 30 tysięcy baryłek ropy. Główny operator ropociągu, firma BP, traciła dziennie 5 milionów dolarów z powodu jego przestoju. Gdy po 19 dniach usunięto uszkodzenia, oszacowano, że sam Azerbejdżan mógł stracić na skutek awarii ok. miliarda dolarów przychodu. Do zamachu natychmiast przyznała się Partia Pracujących Kurdystanu, jednak zdaniem Amerykanów mógł być to efekt porozumienia między rzeczywistymi sprawcami a Kurdami. Amerykanie byli bardzo zainteresowani wyjaśnieniem incydentu, ponieważ był to jeden z pierwszych (jeśli nie pierwszy) przypadek, gdy atak komputerowy doprowadził do fizycznych uszkodzeń infrastruktury krytycznej. Warto pamiętać, że Stuxnet, uznawany za prekursora, rozpoczął swoją niszczycielską działalność dopiero dwa lata później.

Najlepsze w tym miesiącu

- Sony Pictures zhakowane, wszystkie komputery pod kontrolą włamywaczy
- Wersja testowa systemu PKW dostępna publicznie w trybie DEBUG
- Ponad 30 tysięcy plików skradzionych Sony Pictures już w sieci
- Kontrowersyjne nowe narzędzie do wykrywania rządowych trojanów
- To będzie bolało – ponad 100 plików z tysiącami haseł Sony w sieci
- Wybrali z bankomatów małą fortunę, podając odpowiedni kod serwisowy
- I Ty możesz zhakować swój ruter – przykład od Czytelnika

FunSec

- :) Uniwersalna odpowiedź na problemy z bezpieczeństwem
- :) Niektórych zasobów nie da się zabezpieczyć
- :) Ironiczny XSS

Drobiazgi

- Z Sony Pictures wyciekają scenariusze, dane aktorów
- Bezpieczeństwo Google App Engine Java rozbite przez Polaka
- The Pirate Bay wyłączony po nalocie policji
- Jak pisać raporty z pentestów
- Weekendowa Lektura 2014-11-28/2014-12-06

Trzymaj rękę na pulsie

Adres email zapisz

Wyszukiwanie

Szukasz czegoś? szukaj

Atak zaawansowany technologicznie

Dziennikarze Bloomberga dotarli do osób, które prowadziły śledztwo w sprawie awarii. Ich ustalenia rozmijają się z oficjalną wersją. Uszkodzony rurociąg był jednym z lepiej zabezpieczonych. Rury były zakopane pod ziemią, a każdy kilometr instalacji wyposażony był w czujniki ciśnienia, łączące się za pomocą technologii bezprzewodowej z centralą monitoringu. W razie gdyby podstawowa łączność zawiodła, powinien zadziałać awaryjny system łączności satelitarnej. Trasę rurociągu monitorowały również liczne kamery. To one według wyników śledztwa były pierwszym punktem ataku. Błąd w oprogramowaniu je obsługującym pozwolił atakującym na uzyskanie dostępu do wewnętrznej sieci firmy. Następnie włamywacze zlokalizowali komputer zarządzający sygnałami alarmowymi i zainstalowali na nim złośliwe oprogramowanie.

Kolejnym punktem ataku była stacja numer 30. To właśnie jej zaworami sterowali atakujący, by zwiększyć ciśnienie w rurociągu do poziomu powodującego rozszczelnienie, wyciek oraz eksplozję. System sterowania siecią działał w taki sposób, że wystarczyła kontrola nad zaworami jednej stacji, by doprowadzić do katastrofy. Tę teorię potwierdza fakt, że nie znaleziono żadnych śladów ładunków wybuchowych. Włamywaczom udało się także przejąć kontrolę nad systemem monitoringu wideo. Z dysków zniknęło około 60 godzin nagrania z kluczowych lokalizacji krótko przed eksplozją. Włamywacze nie wiedzieli jednak, że jedna z kamer, działająca w podczerwieni, nie była podłączona do głównego rejestratora. Jej nagranie pokazuje dwóch mężczyzn, spacerujących wzdłuż rurociągu z komputerem w ręce krótko przed eksplozją. Obaj mają na sobie ubrania podobne do tych stosowanych przez żołnierzy oddziałów specjalnych. Analiza logów pokazała, że w tym samym momencie, gdy kamera zarejestrowała obecność niezidentyfikowanych osób, miały miejsce próby ataku na infrastrukturę informatyczną.

Trzy dni po wybuchu rozpoczęła się wojna Rosji z Gruzją. Gruziński premier oskarżył wojska rosyjskie o próbę zbombardowania tego samego ropociągu na terenie Gruzji. Atak samolotów – w przeciwieństwie do ataku hakerów – był jednak minimalnie chybiony.

Podobne wpisy

- FBI przejęło podróbki i klony stron w sieci Tor zamiast ich oryginalnych wersji
- Ataki korelacyjne na użytkowników sieci Tor i ich rzeczywista skuteczność
- Wybrali z bankomatów małą fortunę, podając odpowiedni kod serwisowy

Komentarzy: 2

2014.12.11 09:11 Panjapa

Łaziki marsjańskie studentów PB też mają całe mnóstwo błędów w oprogramowaniu ;]

Odpowiedz

2014.12.11 10:13 Robur

„Obaj mają na sobie ubrania podobne do tych stosowanych przez żołnierzy oddziałów specjalnych"- może dorzućcie też, jakiego kraju….

Odpowiedz

Tematy

0day Android Anonymous Apple atak backdoor bitcoin botnet BTC błąd Chiny dane ddos DNS exploit Facebook FBI Google hacked hasła hasło Java konferencja koń trojański kradzież Microsoft narkotyki NSA podsłuch Polska prywatność ruter Silk Road SSL szyfrowanie TOR Twitter tylna furtka USA Weekendowa Lektura wirus wpadka wpadka tygodnia wyciek włamanie