SAD DNS erasoa

BCSC-Erasoa_

SAD_DNS

TLP:WHITE

www.basquecybersecurity.eus

2020ko azaroa

AURKIBIDEA

BCSC-RI buruz 3
Laburpen exekutiboa 4
Azterketa teknikoa 5
Kaltetutako baliabideak 7
Arintzea / Konponbidea 8
Erreferentzia osagarriak 9

Erantzukizunetik salbuesteari buruzko klausula

Honako dokumentu hau eskaintzen da erakundeen eta interesa duten herritarren segurtasunerako, BCSCk beharrezkotzat jotzen dituen alertak ezagutzera emateko. Inongo kasutan BCSC ezin da kontsideratu hemen zabaldutako informazioaren erabilpenak zuzenean nahiz zeharka, ustekabean nahiz modu berezian, eragin litzakeen balizko kalteen arduradun. Gauza bera esan beharra dago BCSCren webean edo hortik esteken bitartez joan litekeen kanpoko web orrialdeetan, sare sozialetan, software produktuetan edo alertan nahiz BCSCren webean agertutako beste edozein informaziotan aipa litezkeen teknologiei dagokienez. Edozein kasutan, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak hemen jasotako terminoetan emandako iritzi eta gomendioak dira eta jakinarazitako informaziotik ezin da ondorioztatu ondorio juridiko loteslerik.

Salmenta debekatzeari buruzko klausula

BCSC-RI BURUZ

Zibersegurtasun Euskal Zentroa (Basque Cybersecurity Centre, BCSC) da Eusko Jaurlaritzak izendatutako entitatea Euskadin zibersegurtasunaren gaian heldutasun maila igotzeko.

Zeharkako ekimena da, Enpresa Garapenerako Euskal Agentziaren (SPRI) barnean kokatua, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren menpe dagoen sozietatea. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile ere: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziazko entitatea da zibersegurtasuna eta konfiantza digitala garatzeko Euskadiko herritar, enpresa eta instituzio publikoen artean, eta batez ere, eskualdeko ekonomiaren sektore estrategikoen kasuan.

Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea, eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, berrikuntza teknologikoaren, ikerkuntzaren, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorretan.

Era berean, hainbat zerbitzu eskaintzen ditu Gertakarien Aurreko Ekipo modura duen rolagatik (aurrerantzean CERT, ingelesezko izenaren siglak direla-eta “Computer Emergency Response Team”). Euskal Autonomia Erkidegoko esparruan mehatxu berriak antzemateko eta horiei buruzko alerta goiztiarrak emateko gaitasuna areagotzen dihardu lanean, informazioaren segurtasun gertakarien erantzunean eta analisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:

LABURPEN EXEKUTIBOA

Kalifornia eta Tsinghuako Unibertsitateetako ikertzaileek DNS protokoloak dituen hainbat segurtasun akatsen berri eman dute, interneteko akats larrienetakotzat izan zen Dan Kaminsky-k aurkitutako akatsaren antzekoak.

2008an Kaminskyk DNS protokoloari eragiten zion ahultasun bat aurkitu zuen, interneteko arkitektura osoan oinarrizkoa zena. Hura baliatuz, erasotzaileek izenen zerbitzariak arriskutan jar zitzaketen helbide batera bidalitako edozein eskaera gune faltsuetara birbideratuz. Eraso hori DNS cache poisoning attack modura ezagutu zen, eta urte horretan bertan argitaratutako partxe batekin arindua izan zen.

Eraso berri honi **“SAD DNS” edo “Side-channel Attacked DNS”** izena eman zaio, eta izen bat ebazteko bezeroak zerbitzariarekin irekitako UDP ataka identifikatzean datza. DNS eskaera bat faltsutzeko erasotzaile batek TXID-a (transakzioaren IDa) eta UDP ataka iturburua ezagutu beharra dauka.

SAD DNSk ICMP erantzunak ez saturatzeko erabiltzen den parametro bat baliatzen du, UDP atakak kontsultatzeko ICMP eskaeren aurrean “ataka itxiaren errorea” erako erantzunen gehieneko muga.

Baliagarriak izan litezkeen hainbat konponbide argitaratu dira, Arintzea / Konponbidea atalean jasotzen direnak.

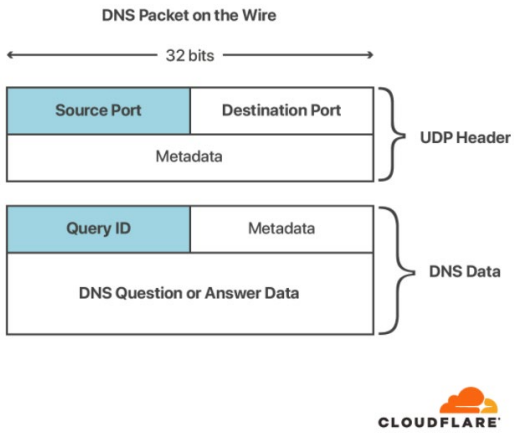
AZTERKETA TEKNIKOA

DNS (Domain Name Systems) protokoloa interneteko funtsezko partea da, izenak IP helbide bihurtzeko lana egiten baitu. Gaur egun, gainera, komunikazioak segurtatzeko ezaugarriak eskaintzen ditu eta TLS ziurtagirien jaulkipenean ezinbestekoa da, gaur egun domeinu izenetara lotuta eskuratzen baitira.

DNS, protokolo bat izateaz gain, sare baten izenekin zerikusia duten datu guztiak erabiltzen dituzten ekipoen hierarkia definitzen duen sistema ere bada.

DNS mezuek UDP garraio protokoloa erabiltzen dute nagusiki eta UDP denez konexiora zuzenduta ez dagoen eta autentifikatuta ez dagoen protokolo bat, edozeinek bidal ditzake erantzunak, erabilitako helbidea eta ataka faltsutuz.

UDPk eskaintzen duen segurtasun faltaren aurrean segurtasuna indartzeko, DNSk bere mezuaren barnean, lehen bi byteetan, Transaction ID (TxID) izeneko eremu bat barneratzen du, eskaeran eta erantzunean berdina izan behar duena:



1. irudia. UDPn kapsulatutako DNS pakete baten azalpena

Honenbestez, erasotzaile batek DNS eskaera bat faltsutu ahal izateko bi datu beharko ditu: bezeroak eskaera egitean zerbitzarian irekitako UDP ataka eta TxID-a, horietako bakoitza 16 biteko tamainakoa. 1. irudian urdinez ikus daitezke bi eremu horiek DNS paketearen barnean. Ondorioz, erasotzaileak arrakasta izateko guztira 32 bit eskuratu behar ditu.

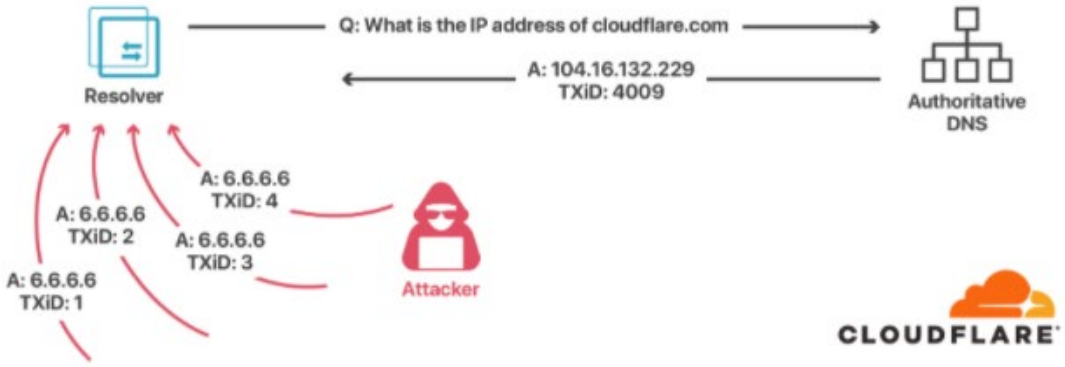
2008an Kaminskyk DNS cache poisoning attack aurkitu aurretik, ebazpen errekurtsiboko sistemek 53. ataka erabili ohi zuten mezuak bidali eta jasotzeko. Hori dela eta, erasotzaile batek asmatu beharra zeukan aldagai bakarra TxID-a osatzen zuten 16 bitak ziren.

DNS cache poisoning attack-ek zuen modua honakoa zen: resolutor errekurtsibo batek domeinu jakin baten izenen zerbitzari baimendua kontsultatzen zuen bitartean, resolutor hori gainezkatu egiten zuen DNS erantzunekin 65 mila (2^{16}) TxID posible baino gehiagoetarako. TxID zuzena zuen asmo gaiztoko erantzuna lehenago iristen bazen baimendutako zerbitzariarena baino, orduan DNSaren cache memoria pozoituta gelditzen zen. Horrela erasotzaileak aukeratutako

erantzun faltsutua itzultzen zen errealaren ordez DNS (TTL) erantzunaren bizitza denboran zehar.

Arazo hori konpontzeko DNS resoluter-etan jatorrizko atakaren ausazkotzea ezartzen hasi zen, eta horrela ez zen aski TxID-a eskuratzea, UDP ataka ere lortu behar zen. Horrekin eraso batek arrakasta izateko aukera dozenaka mila batzuetatik bilioi batera pasa zen ($2^{16}+2^{16}$), eta ondorioz erasoa bideraezina zen.

RFC 5452-n, gainera, DNS sendotzeko eta datuen eskurapena zailtzeko metodoak argitaratu ziren.



2. irudia. DNS cache poisoning attack – Cloudfare

Kalifornia eta Tsinghuako Unibertsitateen argitalpen berriak softwarearen ahultasun baten berri ematen du eta bere azterketa egiten du. **SAD DNS** deitu zaio, (bere ingeleseko siglengatik, **Side-channel Attacked DNS**), DNS azpiegituran erabiltzen den softwarean dago, eta konexiorako erabiltzen den UDP ataka eskuratzea ahalbidetuko luke. Horrek berriz ekarriko luke TxID-a (16 bit) soilik eskuratzea aski den egoera, bi parametroak eskuratu behar izan gabe.

Ataka irekia zein den jakin nahi izanez gero, errazena izango litzateke UDP ataka guztiak eskaneatzea eta ikustea horietatik zein dagoen zabalik. Nolanahi ere horrek denbora gehiegi eramango luke, eta eskaneatzea amaitzerako ataka hori zaharkituta egongo litzateke.

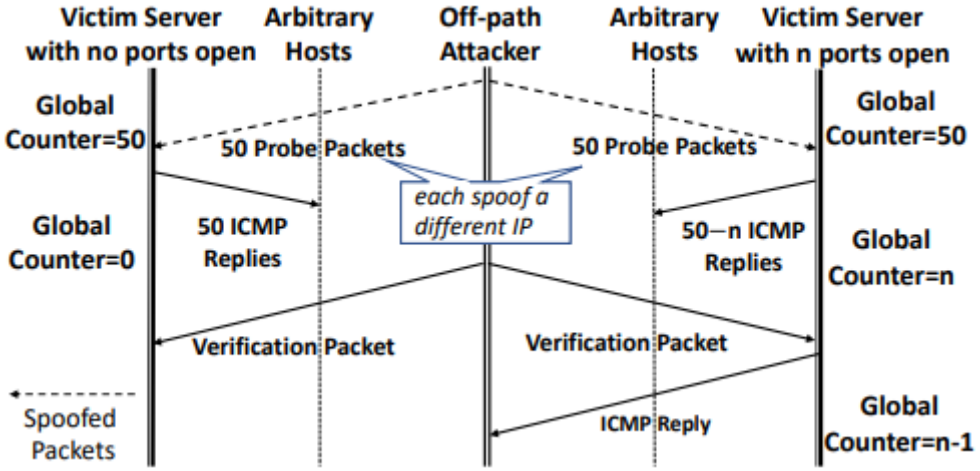
SAD DNS-k erabiltzen duen metodoa baliatu egiten da zerbitzariak “ataka itxiaren errorea” erako ICMP erantzunei ezartzen dien mugaz. Muga hori zerbitzaria saturatzeaz babesteko erabiltzen da, eta gaur egun Sistema Eragile guztietan ezartzen da. Muga horrek finkatzen du “ataka itxiaren errorea” erako zenbat erantzun jasoko den gehienez.

Kalifornia eta Tsinghuako ikertzaileek Linux zerbitzariak aztertu dituzte, askogatik erabilienak direlako. Linuxen bi muga ezartzen zaizkie ICMP errore paketeei, bat orokorra eta beste bat IP bakoitzeko. IPko tasaren muga lehenetsia segundoko 1 da, eta tasa orokorra 1000 (gehienez ere 50 jarraian).

Posible da IP spoofing teknika baliatzea IPko tasa saihesteko eta muga orokorra erabiltzea zunda faltsuek iturburu ataka zuzen bat aurkitu duten edo ez jakiteko

(alegia, “ataka itxiaren errorea” erako erantzunak izan dituzten edo ez), honako urratsak eginez:

1- Gehieneko eskaera kopurua (1000/segundoko) bidaltzen da DNS Resolver biktimarantz faltsututako helbideetatik. Errealki, jarraian 50 soilik bidali ahal izateko mugagatik, 50eko multzotan bidaltzen dira 20 milisegundoro.
2- IP helbideak faltsututa daudenez, erasotzaileak ez ditu erantzunak ikusiko, baina horrek berdin du. Multzo horretarako denbora tartea amaitu aurretik, eskaera bat bidaltzen da edozein UDP atakara, itxita dagoela badakigun batera.
3- “Ataka itxi” erako ICMP errore bat jasotzen bada, horrek esan nahi du ez dela mugara iritsi, eta horrenbestez tarte horretan gutxienez UDP ataka ireki bat zegoela.
4- Horrela, kontsulta sorta batzuen bidez, mugara iristen den edo ez egiaztatuz joaten da, eta horrela ondorioztatzen du zein ataka dauden irekita.



3. irudia. Erasoaren eskema, paper originalean argitaratua.

Kaltetutako baliabideak

Akats honek ondoko sistema eragileei eragiten die: Linux (kernel 3.18-5.10), Windows Server 2019 (1809 bertsioa) eta ondorenekoak, macOS 10.15 eta ondorenekoak, eta FreeBSD 12.1.0 eta ondorenekoak.

Ikertzaileek adierazten dutenez, interneteko DNS zerbitzu garrantzitsuenei eragiten die akatsak, Google eta Cloudfare-ri adibidez, bai eta resolver irekien portzentaje handi bati ere.

ARINTZEA / KONPONBIDEA

SAD DNS erasoaren ondorioak arintzeko hainbat aukera argitaratu dira:

- “Ataka itxia” erako ICMP irteerako mezuak blokeatzea.
- DNSSEC (Domain Name System Security Extensions) erabiltzea, DNS protokoloari integritate eta egiazkotasun konprobazioa gehitzen baitio, eta horrela ordezpen eta faltsutze erako erasoak eragozten dira. DNSSEC ezarrita duten zerbitzariak ez dira ahulak SAD DNS erasoen aurrean. Nolanahi ere, oraingoz DNSSEC-en erabilpena ez dago guztiz zabaldua.

  DNSSEC ezartzeko eta berari buruzko praktika onen gida – Incibe-CERT
- Duela gutxi Linux-en Kernel-aren eguneraketa bat argitaratu da, eraso hau arintzeko zehazki, “ataka itxiaren errorea” erako mezuen tasa orokorraren muga ausazkoak eta aurreikusi ezin direnak erabiltzen dituena.
- Microsoftek 2020ko abenduko ahultasunei buruzko bere buletinean ahultasun honi buruzko Workaround bat jaso du, akatsa saihesteko. Windowsen DNS zerbitzariak 1221eko UDP buffer batekin konfiguratzean datza.

  1. regedit.exe exekutatu administratzaile modura
  2. HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters-en honako parametro hauek sartu:

     Value: MaximunUdpPacketSize

     Type: DWORD

     Data: 4C5 Hexadecimal or 1221 Decimal
  3. Erregistro Editorea itxi eta DNS zerbitzua berrabiatu

  Era horretara, 4C5 edo 1221 baino erantzun handiagoetarako DNS resolver-a TCPra pasatuko litzateke

ERREFERENTZIA OSAGARRIAK

- Azterketaren ikerkuntzaren argitalpena jasotzen duen paper originala – Kalifornia eta Tsinghuako Unibertsitateak
- Cloudfare – SAD DNS Explained
- RFC 5452
- Hackplayers – SAD DNS
- Incibe – DNSSEC Zure web domeinuaren integritatea eta egiazkotasuna ziurtatuz
- Microsoft Guidance for Addressing Spoofing Vulnerability in DNS Resolver

Gertakarien jakinarazpena

Zibersegurtasun gertakariren bat aurkitu baduzu jakinaraz iezaguzu, horrela beharrezkoak diren neurriak hartuko ditugu zabal ez dadin.

900 104 891

arazoak@bcsc.eus

Zibersegurtasun katalogoa

Zure zibersegurtasunarekin edo zure enpresarenarekin laguntza behar duzu?