ئایا دەزانی هێرشی DNS چییە و ئایا تۆرەکەت لە دژی بەهێز کراوە؟

DNS پێش هەموو شتێک بۆ وەڵامدانەوەی دروست و کارا بۆ پرسیارەکان دروستکراوە، نەک پرسیارکردن لە مەبەستەکانیان. لە ئەنجامدا DNS لاوازی و تواناى ڕاستەقینەی هەیە وەک ڤێکتەرێک بۆ هێرشە ئەلیکترۆنییەکان. هێرشی سیستەمی ناوی دۆمەین (DNS) هێرشێکە کە ئەکتەرێکی خراپ یان هەوڵدەدات سازش بە DNS ی تۆڕێک بکات یان سوود لە تایبەتمەندییە سروشتییەکانی وەردەگرێت بۆ ئەنجامدانی هێرشێکی فراوانتر. هێرشێکی DNS کە بە باشی ڕێکخراوە دەتوانێت ڕێکخراوێک بخاتە سەر ئەژنۆی خۆی.

ئەم پۆستە ورد دەبێتەوە لە چوار جۆری سەرەکی هێرشی DNS. دواتر باس لە هەنگاوە سەرەتاییەکان دەکات کە دەتوانیت بیگریتە بەر بۆ ڕێگریکردن لە هێرشی DNS.

جۆرە سەرەکییەکانی هێرشی DNS

هێرشی DNS ژێرخانی DNS دەکاتە ئامانج. دەتوانرێت هێرشەکان بۆ سێرڤەرە دووبارەبووەکان یان دەسەڵاتدارەکان داڕێژرێت. چوار جۆری سەرەکی هێرش هەیە کە DNS بەکاردەهێنن.

هێرشی گەورەکردنی DoS و DDoS و هێرشی ڕەتکردنەوەی خزمەتگوزاری (DoS) و هێرشی ڕەتکردنەوەی خزمەتگوزاری دابەشکراو (DDoS) دوو جۆری هەمان شتن. ئەوان ئەو شتانەن کە زۆربەی خەڵک بیریان لێدەکەنەوە کاتێک بیر لە هێرشی DNS دەکەنەوە. لە هەردوو حاڵەتەکەدا هێرشبەران بە داواکاری زۆرەوە سێرڤەرەکانی ئینتەرنێت لافاو دەدەن کە بە سادەیی ناتوانن وەڵامی هەموویان بدەنەوە و لە ئەنجامدا سیستەمەکە نێکدەچێت.

هێرشی ڕەتکردنەوەی خزمەتگوزاری (DoS)

هێرشێکی سادەی DoS یەک کۆمپیوتەر و یەک هێڵی ئینتەرنێت بەکاردەهێنێت بۆ لافاوکردنی سێرڤەرێکی دوور. ئەوان بە شێوەیەکی ترسناک کاریگەر نین لە سەرکوتکردنی سیستەمی توانای بەرزی ئەمڕۆ.

هێرشی ڕەتکردنەوەی خزمەتگوزاری دابەشکراو (DDoS)

لە هێرشی DDoS دا چەندین کۆمپیوتەر و هێڵی ئینتەرنێت سایتێک دەکەنە ئامانج. زۆرجار، هێرشەکانی DDoS کۆمپیوتەرە مەترسیدارەکان زیاد دەکەن بۆ بۆتنێتێک کە پرسیارە زیانبەخشەکان لە پاشبنەمادا بەڕێوەدەبات. هێرشبەران دەتوانن هێزی ئامێرەکانی جیهان بەکاربهێنن بۆ ئەوەی بە یەکجار پرسیار لە تۆری ئامانج بکەن.

هەروەها سێ جۆری لاوەکی هێرشی DDoS هەیە:

هێرشی پرۆتۆکۆڵ: ئەم هێرشە سەرچاوەی ڕاستەقینەی سێرڤەر یان ئامێرەکانی تری تۆر وەک دیواری ئاگرین و لۆد باڵانسەر پەک دەخات.

هێرشەکانی چینەکانی بەرنامە: بۆ نێکدانی سێرڤەری وێب، هێرشبەرەکە داواکاری دەنێرێت کە پێدەچێت بێ زیان بێت بەڵام لە ڕاستیدا لاوازییەکانی ئامانجەکە دەقۆزێتەوە.

هێرشی لافاو: ئامانجی لافاوەکان ئەوەیە کە سێرڤەرێک لەبەردەستی ترافیکی ڕاستەقینەدا بەردەست نەبێت بە لافاوکردنی سەرچاوەکانی سێرڤەری ئامانجدار.

لە ڕاســـتیدا، هێرشـــەکانی DDoS زۆرجار چینە تایبەتەکانی مۆدێلی OSI دەکەنە ئامانج. مۆدێلەکە پەیوەندیکردن لە ســـەرانســـەری تۆڕەکانی کۆمپیوتەردا دابەش دەکات بۆ حەوت چینە ئەبســـتراکت کە هەریەکەیان ئەرکێکی جیاواز لە پەیوەندی تۆڕەکاندا ئەنجام دەدەن.

لە شـــوباتی ٢٠٢٠، خزمەتگوزاری AWS Shield ی ئەمازۆن گەورەترین هێرشـــی DDoS ی تا ئێســـتا (2.3 Tbps) پووچەڵکردەوە، کە بە بەکارهێنانی وێب ســـێرڤەرە ڕفێنراوەکانی Connection-less Lightweight Directory Access Protocol ئەنجامدرا.

هێرشەکانی گەورەکردنی DNS

جگە لەوەش، هێرشـی گەورەکردنی DNS جۆرێکە لە هێرشـی DDoS کە هێرشـبەران سـێرڤەرە کراوەکانی DNS بەکاردەهێنن کە بە ئاشکرا دەستیان پێدەگات بۆ لافاوکردنی ئامانجێک بە ترافیکی وەڵامی DNS.

هێرشبەرێک داواکاری گەڕانی DNS دەنێرێت بۆ سێرڤەرێکی DNS کراوە کە ناونیشانی سەرچاوەکە ساختە کراوە بۆ ئەوەی ناونیشـــانی ئامانجەکە بێت. کاتێک کە ڕاژەکاری DNS وەڵامی تۆماری DNS دەنێرێت، لەبری ئەوە دەنێردرێت بۆ ئامانج.

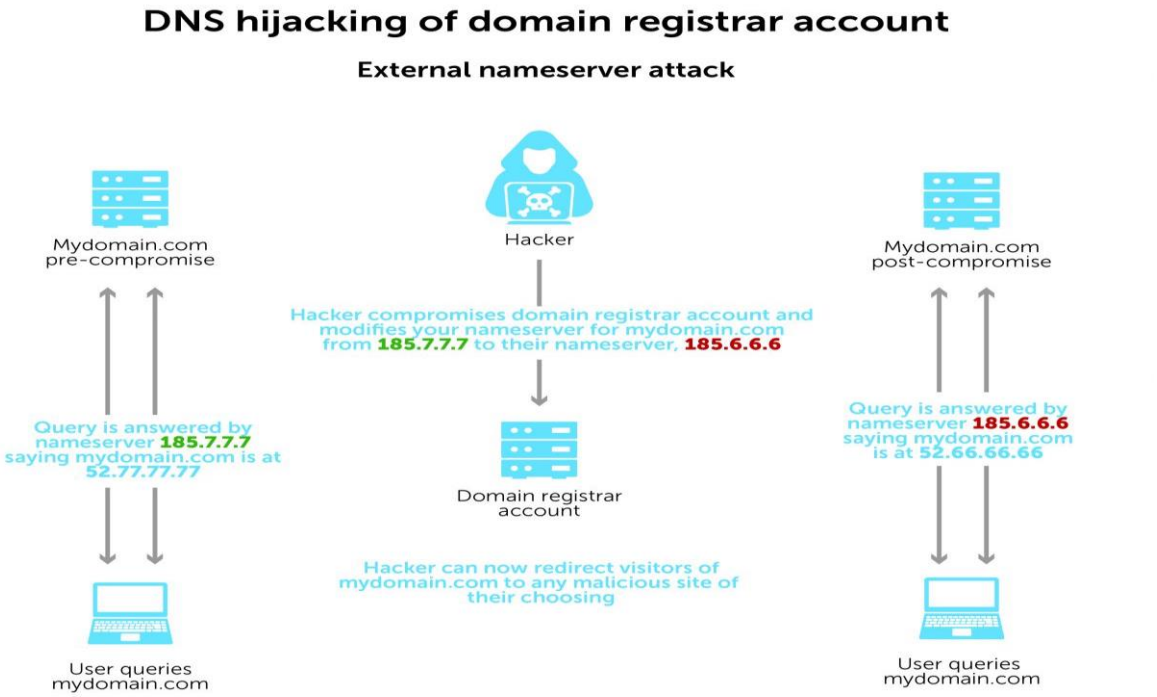
هایجاککردنی DNS

سێ جۆر DNS هایجاککردن هەیە:

- هێرشـبەران دەتوانن سـازش بە ئەکاونتی تۆمارکەری دۆمەین بکەن و دەسـتکاری ناوی DNS بکەن بۆ ئەوەی کە ئەوان کۆنترۆڵی دەکەن (پروانە وێنەکە).
- ئەکتەرە خراپەکان دەتوانن تۆماری A بۆ ناونیشـانی IP ی دۆمەینەکەت بگۆڕن بۆ ئەوەی لەبری ئەوە ئاماژە بە ناونیشانەکەیان بکات.

Cyber Shield

- هێرشـــبەران دەتوانن ســـازش بە ڕاوتەڕێکی ڕێکخراوێک بکەن و ســـێرڤەری DNS بگۆڕن کە بە شـــێوەیەکی ئۆتۆماتیکی پاڵدەنرێتە خوارەوە بۆ هەر ئامێرێـک کـاتێـک بەکـارهێنەران دەچنە نـاو تۆرەکەتەوە.



لە ســـاڵی ٢٠١٩ شـــارەزایانی بواری ئەمنی، ســـی تورتلیان دۆزییەوە کە هەڵمەتێکی ڕفاندنی DNS بە سـپۆنسـەری دەوڵەتە و دەسـتکاری تۆماری DNSی لانیکەم ٤٠ ڕێکخراوی لە ١٣ وڵاتدا کردووە و سـاختەی کردووە.

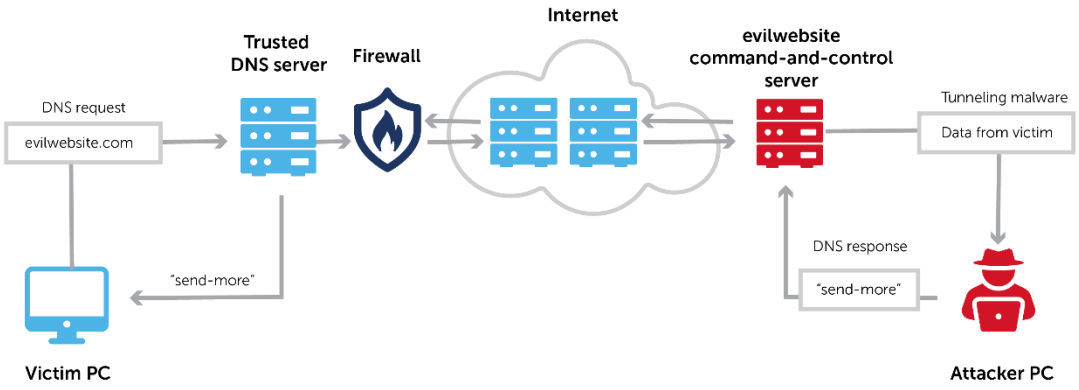
تونێلکردنی DNS

تونێلکردنی DNS زانیاری لە ڕێگەی پرۆتۆکۆڵی DNS دەگوازێتەوە کە بەزۆری ناونیشـانی تۆرەکان چارەسـەر دەکات.

داواکاری ئاسـایی DNS تەنها ئەو زانیاریانە لەخۆدەگرێت کە پێویسـتن بۆ پەیوەندیکردن لە نێوان مشـتەری و سـێرڤەر. تونێلکردنی DNS ڕیزێکی زیـادەی داتـا دەخـاتە نـاو ئەو ڕێرەوەوە. فۆرمێکی پەیوەنـدیکردن دادەمەزرێنێت کە زۆربەی فلتەرەکان و دیواری ئاگرین و نەرمەکاڵاکانی گرتنی پاکەتەکان بەدەر دەکات.

ئەمەش وا دەکات بە تایبەتی دەسـتنیشـانکردن و شـوێنپێهەڵگرتنی سـەرچاوەکەی قورس بێت. تونێلکردنی DNS دەتوانێت فەرمان و کۆنترۆڵ دابنێت. یان، دەتوانێت داتاکان دەربهێنێت. زۆرجار زانیارییەکان دابەش دەکرێن بۆ پارچەی بچووکتر، بە درێژایی DNS دەجوڵێن و لە کۆتاییەکەی تردا کۆدەکرێنەوە.

DNS tunneling



ژەهراویبوونی DNS و ژەهراویبوونی کاش

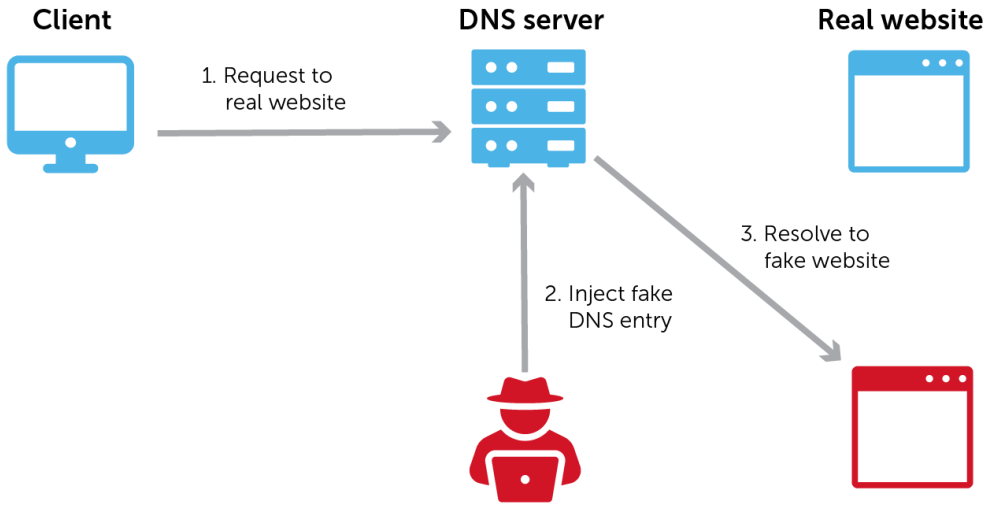
ژەهراویبوونی DNS (کە بە DNS spoofing ناسـراوە) و ئامۆزاکەی کە ژەهراویبوونی DNS cache، بۆشـایی ئەمنی لە پرۆتۆکۆڵی DNS بەکـاردەهێنن بۆ ئـاڕاســتەکردنەوەی هـاتوچۆی ئینتەرنێـت بۆ مـاڵپەڕە زیانبەخشەکان. ئەمانە هەندێک جار پێیان دەوترێت هێرشی پیاوی ناوەڕاست.

کاتێک وێبگەڕەکەت دەچێتە دەرەوە بۆ ئینتەرنێت، بە داواکردن لە سێرڤەرێکی DNS ناوخۆیی دەست پێدەکات بۆ دۆزینەوەی ناونیشـانی IP بۆ ناوی ماڵپەڕێک. ڕاژەکاری DNS ناوخۆیی پرسـیار لەو سـێرڤەرە ڕەگانە دەکات کە خاوەنی ئەو دۆمەینەن، و پاشـــان پرســـیار لە ڕاژەکاری ناوی دەســـەڵاتداری ئەو دۆمەینە دەکات بۆ ناونیشانەکە.

ژەهراویبوونی DNS کاتێک ڕووەدات کە ئەکتەرێکی زیانبەخش دەستوەردان لەو پرۆسەیەدا بکات و وەڵامی هەڵە دابین بکات. کاتێک فێڵی لە وێبگەڕەکەی کرد و پێیوابوو وەڵامی دروسـتی بۆ پرسـیارەکەی وەرگرتووە، ئەو ئەکتەرە زیانبەخشە دەتوانێت ترافیکی بگۆڕێت بۆ هەر ماڵپەڕێکی ساختە کە بیەوێت.

Cyber Shield

DNS poisoning



لە ژەهراویبوونی DNS cache دا، کاتێک ئەکتەرێکی زیانبەخش پرسیارێکی DNS دەگۆڕێت و 'وڵامی' دەداتەوە، چارەسەرکەری DNS ئەو وەڵامانە لە کاشێکدا هەڵدەگرێت بۆ بەکارهێنانی لە داهاتوودا. (زۆربەی چارەسەرکەرانی DNS چارەسەرکەری کاشین.) لەم حاڵەتەدا، هێرشەکە خراپتر دەکات بە بەردەوامبوون لە دابینکردنی ئەو وەڵامە هەڵەیە.

چەند کاتژمێر ئەو نووسراوانەی DNS لە کاشەکەتدا دەمێننەوە، بەندە بە کاتی ژیانەوە (TTL). ئەمە ڕێکخستنێکی ڕاژەکاری DNS یە کە بە کاشەکە دەڵێت کە چەند کاتژمێر تۆمارەکانی DNS هەڵبگرێت پێش ئەوەی گەڕان بۆ سێرڤەرێکی یاسایی نوێ بکاتەوە.

لە تشرینی دووەمی ٢٠٢٠ توێژەران ڕێگەیەکی نوێیان بۆ ئەنجامدانی ژەهراویکردنی کاش ئاشکرا کرد، کە ناوی SAD DNS (کورتی Side-channel AttackeD DNS)ە. شێوازەکە ڕێگە بە هێرشبەر دەدات کەناڵێکی لاوەکی بەکاربهێنێت بۆ دەرزی لێدانی تۆمارێکی DNS زیانبەخش بۆ ناو کاشی DNS.

چۆنێتی ڕێگریکردن و دەستنیشانکردن و کەمکردنەوەی هێرشی DNS

لە کاتێکدا کە DNS لە مێژوودا وەک پیاوێکی بێهەڵوێست سەیر کراوە، بەڵام دەتوانێت بەشێکی چالاکانە بێت لە ستراتیژییەکی باشی بەرگریکردن-بە قووڵی. گارتنەر لەگەڵ دەزگا دیارەکانی حکومەتی ئەمریکا وەک NSA، دواجار بەم دواییە ئاسایشی DNSیان بە گرنگ ناساند بۆ باشترکردنی بەرگری گشتی تۆرەکەت.

ئێستا چەمکی DNS ی پارێزەر بوونی هەیە بۆ وەسفکردنی DNS بە گرنگ بۆ پاراستن لە هەڕەشەکانی تۆر.

لێرەدا چەند هەنگاوێکی بنەڕەتی پارێزەر دەخەینەڕوو:

تەواوی بیناسازی DNS ی خۆت بناسە. بۆ دەستپێکردن، پاراستنی توڕێک پێویستی بە هۆشیاری هەیە لە تەواوی DNS ی کۆمپانیاکەتان. زۆرجار، تیمەکانی تۆر بەهۆی فەسادی سایلۆکانی DNS، بە بێ سەرپەرشت، یان ئایتی سێبەرەوە، بینینی تەواویان نییە.

لۆگکردن و چاودێریکردنی پرسیارەکانی DNS و داتاکانی وەڵامدانەوە. تۆمارکردن و چاودێریکردنی پرسیارەکانی دەرەوە و هاتوو یەکەم هەنگاوە بۆ دیاریکردنی ناتەواوییەکان. سەرەڕای ئەوە، داتاکانی وەڵامدانەوەی تۆ زانیاری کۆنتێکست دەدات کە ڕێگە بە شیکارییەکی پزیشکی دادوەری وردتر دەدات.

سێرڤەرە دووبارەبووەکانی DNS هەکانت ڕەق بکەرەوە. پاراستنی سێرڤەرە دووبارەبووەکان لە دەستڕاگەیشتن و دەستکاریکردنی نەخوازراو لە ڕێگەی DNSSEC، کۆنترۆڵەکانی دەستڕاگەیشتن و باشترکردنی بیناسازییەکانی تر.

دەستڕاگەیشتن بە بەڕێوەبەر بۆ DNS کەت توند بکەرەوە. ڕەسەنایەتی فرە فاکتەری لەسەر ئەژمێری تۆمارکەری دۆمەینەکەت چالاک بکە و خزمەتگوزاری قوفڵی تۆمارکەر بەکاربهێنە بۆ داوای مۆڵەتەکەت پێش گۆڕینی تۆمارەکانی DNS.

نوسینی بابەت و چاکردن پێداچونەوە

Heisenberg And Ahmed Abdalkhaliq Abdulla

Cyber Shield

https://www.youtube.com/@cybershieldteam

/https://www.facebook.com/groups/409441013446196

/https://www.facebook.com/cybershield.team