

Ad: Meryem Idris

No: 170504068

Ad: Mehmet Fevzi Canbek

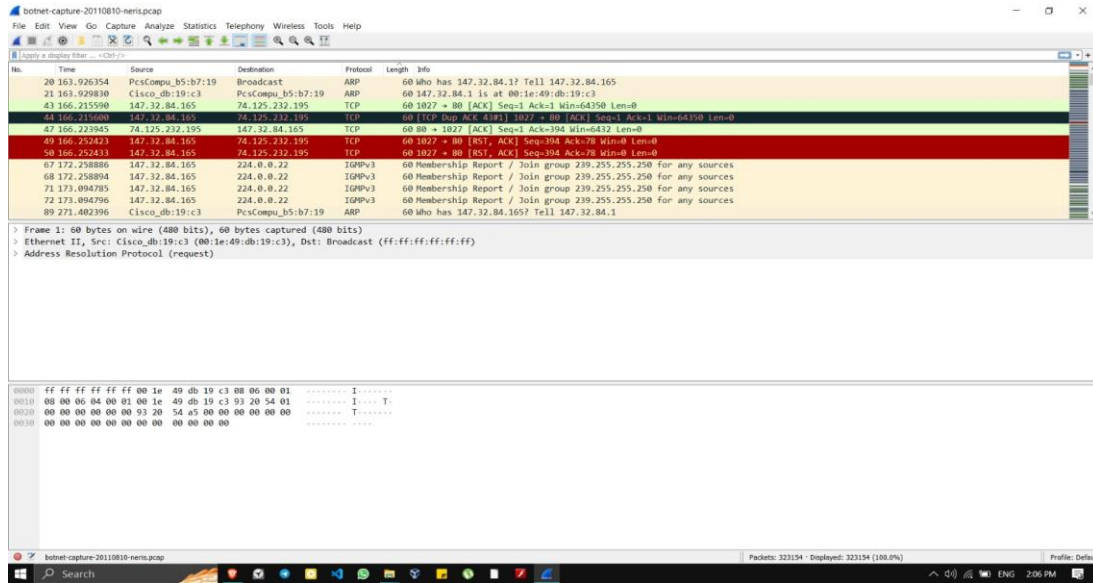
No: 190504103

CTU-13 Veri Kümesi hakkında bilgi

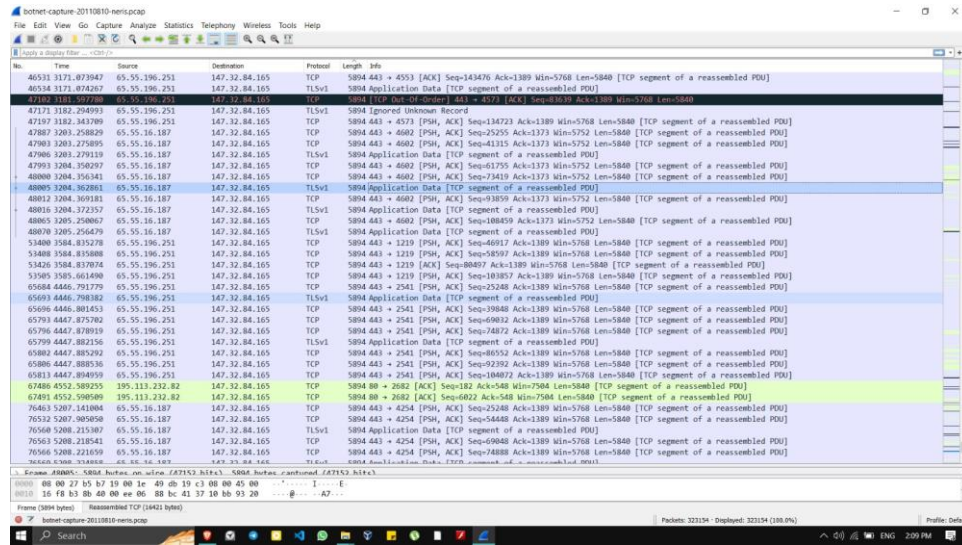
CTU-13 veri seti, çek cumhuriyeti'ndeki CTU üniversitesinde Stratosfer Laboratuvarı tarafından toplanan ağ trafiği verilerinden derlenmiştir.

Amaç: Veriler, siber güvenliğe ilişkin ağ trafiğinin analizi, kötü amaçlı ağ faaliyetlerinin tespit edilmesi ve siber güvenlik tehditlerinin araştırılmasının kolaylaştırılması amacıyla toplanır.

Siber Güvenlikle İlgisi: Veri kümesi, kötü amaçlı yazılım tespitini, ağ saldırılarını ve çeşitli siber güvenlik tehditlerini incelemek için gerekli olan ağ trafiği verilerini sağlar.



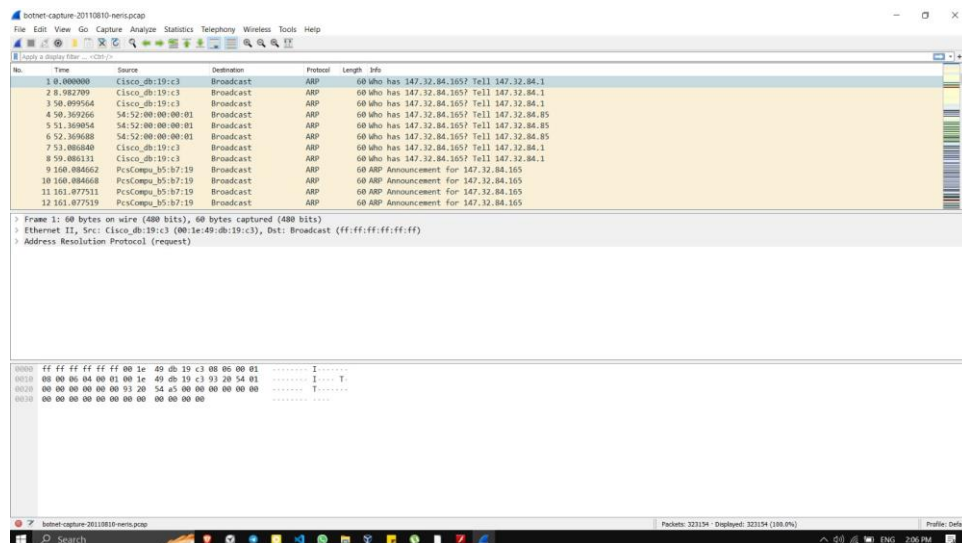
Veri Ön İşleme



The image shows a Wireshark packet capture of a Denial of Service (DoS) attack. The packet list on the left shows a series of SYN packets from source IP 192.168.1.100 to destination IP 192.168.1.1. The packet details pane on the right shows the structure of a TCP segment, including the source and destination ports, sequence number, and flags. The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header, Internet Protocol header, and Transmission Control Protocol header.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-------------|----------------|---------------|----------|--------|--|
| 40531 | 1371.073947 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 4553 [ACK] Seq=143476 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 40534 | 1371.074297 | 65.55.196.251 | 147.32.84.165 | TLSv1 | 5804 | Application Data [TCP segment of a reassembled PDU] |
| 47382 | 1381.597780 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | [TCP Out-of-Order] 443 → 4573 [ACK] Seq=43619 Ack=1389 Win=5768 Len=5840 |
| 47171 | 1382.254993 | 65.55.196.251 | 147.32.84.165 | TLSv1 | 5804 | Ignored Unknown Record |
| 47197 | 1382.343798 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 4573 [PSH, ACK] Seq=14723 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 47887 | 1383.258829 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4602 [PSH, ACK] Seq=25255 Ack=1373 Win=5752 Len=5840 [TCP segment of a reassembled PDU] |
| 47903 | 1383.275895 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4602 [PSH, ACK] Seq=41315 Ack=1373 Win=5752 Len=5840 [TCP segment of a reassembled PDU] |
| 47986 | 1383.279119 | 65.55.16.187 | 147.32.84.165 | TLSv1 | 5804 | Application Data [TCP segment of a reassembled PDU] |
| 47993 | 1384.356297 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4602 [PSH, ACK] Seq=41729 Ack=1373 Win=5752 Len=5840 [TCP segment of a reassembled PDU] |
| 48000 | 1384.356341 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4602 [PSH, ACK] Seq=73419 Ack=1373 Win=5752 Len=5840 [TCP segment of a reassembled PDU] |
| 48003 | 1384.362881 | 65.55.16.187 | 147.32.84.165 | TLSv1 | 5804 | Application Data [TCP segment of a reassembled PDU] |
| 48012 | 1384.365181 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4602 [PSH, ACK] Seq=93859 Ack=1373 Win=5752 Len=5840 [TCP segment of a reassembled PDU] |
| 48016 | 1384.372357 | 65.55.16.187 | 147.32.84.165 | TLSv1 | 5804 | Application Data [TCP segment of a reassembled PDU] |
| 48005 | 1385.250867 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4602 [PSH, ACK] Seq=108459 Ack=1373 Win=5752 Len=5840 [TCP segment of a reassembled PDU] |
| 48010 | 1385.256479 | 65.55.16.187 | 147.32.84.165 | TLSv1 | 5804 | Application Data [TCP segment of a reassembled PDU] |
| 53480 | 1584.835278 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 1219 [PSH, ACK] Seq=46917 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 53488 | 1584.835808 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 1219 [PSH, ACK] Seq=58597 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 53426 | 1584.837074 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 1219 [ACK] Seq=80807 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 53505 | 1585.061490 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 1219 [PSH, ACK] Seq=103857 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 65084 | 4446.791779 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 2541 [PSH, ACK] Seq=25248 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 65093 | 4446.798382 | 65.55.196.251 | 147.32.84.165 | TLSv1 | 5804 | Application Data [TCP segment of a reassembled PDU] |
| 65096 | 4446.801453 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 2541 [PSH, ACK] Seq=39648 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 65793 | 4447.875782 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 2541 [PSH, ACK] Seq=69832 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 65796 | 4447.878919 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 2541 [PSH, ACK] Seq=74872 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 65799 | 4447.882156 | 65.55.196.251 | 147.32.84.165 | TLSv1 | 5804 | Application Data [TCP segment of a reassembled PDU] |
| 65802 | 4447.885292 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 2541 [PSH, ACK] Seq=86552 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 65806 | 4447.888536 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 2541 [PSH, ACK] Seq=92392 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 65813 | 4447.894919 | 65.55.196.251 | 147.32.84.165 | TCP | 5804 | 443 → 2541 [PSH, ACK] Seq=104872 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 67486 | 4552.589255 | 195.113.232.82 | 147.32.84.165 | TCP | 5804 | 80 → 2682 [ACK] Seq=182 Ack=548 Win=7504 Len=5840 [TCP segment of a reassembled PDU] |
| 67491 | 4552.590540 | 195.113.232.82 | 147.32.84.165 | TCP | 5804 | 80 → 2682 [ACK] Seq=6822 Ack=548 Win=7504 Len=5840 [TCP segment of a reassembled PDU] |
| 76463 | 5207.141004 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4254 [PSH, ACK] Seq=25248 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 76532 | 5207.909580 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4254 [PSH, ACK] Seq=54448 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 76568 | 5208.215187 | 65.55.16.187 | 147.32.84.165 | TLSv1 | 5804 | Application Data [TCP segment of a reassembled PDU] |
| 76563 | 5208.218541 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4254 [PSH, ACK] Seq=69848 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 76566 | 5208.221659 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4254 [PSH, ACK] Seq=74888 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |
| 76568 | 5208.224808 | 65.55.16.187 | 147.32.84.165 | TCP | 5804 | 443 → 4254 [PSH, ACK] Seq=80888 Ack=1389 Win=5768 Len=5840 [TCP segment of a reassembled PDU] |

Geleneksel Hizmet Reddi (DoS) saldırılarının aksine, uygulama katmanı DoS saldırıları ağ katmanında neredeyse tespit edilemez. CIC DoS, uygulama katmanı DoS saldırılarını içeren izinsiz giriş tespit veri kümelerinden biridir. Bu nedenle bu çalışmada Rastgele Orman, Extreme Gradient Boosting (XGBoost), Light Gradient Boosting Machine (LGBM), Gradient Boosting, Multilayer Perceptron (MLP), Evrişimli Sinir Ağları (CNN) kullanarak uygulama tabanlı DoS saldırılarını tespit etmek için bu veri setini ele aldık.ve Destek Vektör Makinesi (SVM) algoritmaları. Deneyisel sonuçlar, LGBM tabanlı modelin performansının diğer algoritmalara göre daha iyi olduğunu göstermektedir.



The image shows a Wireshark packet capture of a Denial of Service (DoS) attack. The packet list on the left shows a series of ARP requests and responses from source IP 192.168.1.100 to destination IP 192.168.1.1. The packet details pane on the right shows the structure of an ARP request, including the source and destination MAC addresses, source and destination IP addresses, and the ARP operation code. The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header, Internet Protocol header, and ARP header.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------------|-------------|----------|--------|---|
| 1 | 0.000000 | Cisco_OB:19:c3 | Broadcast | ARP | 60 | Who has 147.32.84.165? Tell 147.32.84.1 |
| 2 | 0.000000 | Cisco_OB:19:c3 | Broadcast | ARP | 60 | Who has 147.32.84.165? Tell 147.32.84.1 |
| 3 | 0.000000 | Cisco_OB:19:c3 | Broadcast | ARP | 60 | Who has 147.32.84.165? Tell 147.32.84.1 |
| 4 | 0.000000 | 54:52:00:00:00:01 | Broadcast | ARP | 60 | Who has 147.32.84.165? Tell 147.32.84.1 |
| 5 | 0.000000 | 54:52:00:00:00:01 | Broadcast | ARP | 60 | Who has 147.32.84.165? Tell 147.32.84.1 |
| 6 | 0.000000 | 54:52:00:00:00:01 | Broadcast | ARP | 60 | Who has 147.32.84.165? Tell 147.32.84.1 |
| 7 | 0.000000 | Cisco_OB:19:c3 | Broadcast | ARP | 60 | Who has 147.32.84.165? Tell 147.32.84.1 |
| 8 | 0.000000 | Cisco_OB:19:c3 | Broadcast | ARP | 60 | Who has 147.32.84.165? Tell 147.32.84.1 |
| 9 | 0.000000 | PcsComp_35:b7:19 | Broadcast | ARP | 60 | ARP Announcement for 147.32.84.165 |
| 10 | 0.000000 | PcsComp_35:b7:19 | Broadcast | ARP | 60 | ARP Announcement for 147.32.84.165 |
| 11 | 0.000000 | PcsComp_35:b7:19 | Broadcast | ARP | 60 | ARP Announcement for 147.32.84.165 |
| 12 | 0.000000 | PcsComp_35:b7:19 | Broadcast | ARP | 60 | ARP Announcement for 147.32.84.165 |

Wireshark capture of botnet traffic (20110810-netscap). The capture shows several ARP and TCP packets. The ARP packets are from 192.168.1.102 to 192.168.1.103. The TCP packets are from 192.168.1.102 to 192.168.1.103. The packets are captured on the interface eth0.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|-------------------|----------------|----------|--------|---|
| 90 | 271.402693 | PcsCompu_b5:b7:19 | Cisco_db:19:c3 | ARP | 60 | 147.32.84.165 is at 08:00:27:b5:b7:19 |
| 91 | 271.402702 | PcsCompu_b5:b7:19 | Cisco_db:19:c3 | ARP | 60 | 147.32.84.165 is at 08:00:27:b5:b7:19 |
| 98 | 282.408448 | 147.32.84.165 | 60.190.222.139 | TCP | 60 | 1809 → 65520 [ACK] Seq=1 Acks=1 Win=64240 Len=0 |
| 99 | 282.408457 | 147.32.84.165 | 60.190.222.139 | TCP | 60 | TCP Dup ACK 98(1) 1035 → 65520 [ACK] Seq=1 Acks=1 Win=64240 Len=0 |
| 182 | 283.291529 | 60.190.222.139 | 147.32.84.165 | TCP | 60 | 65520 → 1809 [ACK] Seq=1 Acks=21 Win=5840 Len=0 |
| 185 | 283.597149 | 60.190.222.139 | 147.32.84.165 | TCP | 60 | 65520 → 1809 [ACK] Seq=1 Acks=20 Win=5840 Len=0 |
| 187 | 285.546878 | 147.32.84.165 | 60.190.222.139 | TCP | 60 | 1809 → 65520 [ACK] Seq=70 Acks=250 Win=63991 Len=0 |
| 188 | 285.546888 | 147.32.84.165 | 60.190.222.139 | TCP | 60 | TCP Dup ACK 187(1) 1830 → 65520 [ACK] Seq=70 Acks=250 Win=63991 Len=0 |
| 221 | 295.637929 | 147.32.84.165 | 94.63.149.152 | TCP | 60 | 1809 → 80 [ACK] Seq=1 Acks=1 Win=64240 Len=0 |
| 222 | 295.637938 | 147.32.84.165 | 94.63.149.152 | TCP | 60 | TCP Dup ACK 221(1) 1808 → 80 [ACK] Seq=1 Acks=1 Win=64240 Len=0 |
| 125 | 295.673716 | 94.63.149.152 | 147.32.84.165 | TCP | 60 | 80 → 1808 [ACK] Seq=1 Acks=91 Win=5840 Len=0 |
| 127 | 295.675997 | 147.32.84.165 | 94.63.149.152 | TCP | 60 | 1808 → 80 [ACK] Seq=91 Acks=221 Win=64240 Len=0 |

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, Src: Cisco_db:19:c3 (00:1e:4d:0b:19:c3), Dst: Broadcast (ff:ff:ff:ff:ff:ff).
Address Resolution Protocol (request)

Keşif Amaçlı Veri Analizi (EDA)

Wireshark capture of botnet traffic (20110810-netscap). The capture shows several TCP segments of a reassembled PDU. The segments are from 192.168.1.102 to 192.168.1.103. The packets are captured on the interface eth0.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|----------------|---------------|----------|--------|---|
| 2596 | 1481.017564 | 65.55.16.187 | 147.32.84.165 | TLSv1 | 4434 | Application Data [TCP segment of a reassembled PDU] |
| 2596 | 1481.017564 | 65.55.16.187 | 147.32.84.165 | TCP | 4434 | 443 → 4004 [ACK] Seq=90948 Acks=1389 Win=5768 Len=4380 [TCP segment of a reassembled PDU] |
| 2605 | 14851.351662 | 65.54.234.75 | 147.32.84.165 | TCP | 4434 | 443 → 4775 [ACK] Seq=7945 Acks=1181 Win=63269 Len=4380 [TCP segment of a reassembled PDU] |
| 2618 | 14878.772987 | 195.113.232.99 | 147.32.84.165 | TCP | 4434 | 80 → 1141 [ACK] Seq=5841 Acks=400 Win=6432 Len=4380 [TCP segment of a reassembled PDU] |
| 2611 | 14878.774236 | 195.113.232.99 | 147.32.84.165 | TCP | 4434 | 80 → 1141 [ACK] Seq=23161 Acks=400 Win=6432 Len=4380 [TCP segment of a reassembled PDU] |
| 2611 | 14878.775232 | 195.113.232.99 | 147.32.84.165 | TCP | 4434 | 80 → 1141 [ACK] Seq=27741 Acks=400 Win=6432 Len=4380 [TCP segment of a reassembled PDU] |
| 2668 | 15136.266811 | 65.55.16.187 | 147.32.84.165 | TCP | 4434 | 443 → 4050 [ACK] Seq=25017 Acks=1389 Win=5768 Len=4380 [TCP segment of a reassembled PDU] |
| 2661 | 15136.808758 | 65.55.16.187 | 147.32.84.165 | TCP | 4434 | 443 → 4050 [PSH, ACK] Seq=41877 Acks=1389 Win=5768 Len=4380 [TCP segment of a reassembled PDU] |
| 2662 | 15137.527747 | 65.55.16.187 | 147.32.84.165 | TLSv1 | 4434 | Application Data [TCP segment of a reassembled PDU] |
| 2662 | 15137.977141 | 65.55.16.187 | 147.32.84.165 | TLSv1 | 4434 | Application Data [TCP segment of a reassembled PDU] |
| 2662 | 15138.417495 | 65.55.16.187 | 147.32.84.165 | TLSv1 | 4434 | Application Data [TCP segment of a reassembled PDU] |
| 2662 | 15138.428955 | 65.55.16.187 | 147.32.84.165 | TCP | 4434 | 443 → 4050 [PSH, ACK] Seq=121377 Acks=1389 Win=5768 Len=4380 [TCP segment of a reassembled PDU] |
| 2668 | 15155.609968 | 174.36.246.56 | 147.32.84.165 | TCP | 4434 | 80 → 1533 [ACK] Seq=5817 Acks=379 Win=6432 Len=4380 [TCP segment of a reassembled PDU] |
| 2674 | 15163.712021 | 195.113.232.82 | 147.32.84.165 | TCP | 4434 | 80 → 1552 [ACK] Seq=6022 Acks=481 Win=7984 Len=4380 [TCP segment of a reassembled PDU] |
| 2674 | 15163.715255 | 195.113.232.82 | 147.32.84.165 | TCP | 4434 | 80 → 1552 [ACK] Seq=33762 Acks=481 Win=7984 Len=4380 [TCP segment of a reassembled PDU] |

Frame 26187: 4434 bytes on wire (35472 bits), 4434 bytes captured (35472 bits) on interface eth0, Src: Cisco_db:19:c3 (00:1e:4d:0b:19:c3), Dst: PcsCompu_b5:b7:19 (08:00:27:b5:b7:19).
Ethernet II, Src: Cisco_db:19:c3 (00:1e:4d:0b:19:c3), Dst: PcsCompu_b5:b7:19 (08:00:27:b5:b7:19)
Internet Protocol Version 4, Src: 195.113.232.99, Dst: 147.32.84.165
Transmission Control Protocol, Src Port: 80, Dst Port: 1141, Seq: 23161, Acks: 400, Len: 4380

261107: Yakalama aracının pakete atadığı paket numarası veya sıra numarasıdır.

14878.774236: Paketin ne zaman yakalandığını belirten, yakalamanın başlangıcından bu yana geçen süreyi saniye cinsinden temsil eder.

195.113.232.99: Paketin kaynağının veya göndericisinin IP adresidir.

147.32.84.165: Paketin hedef veya alıcısının IP adresidir.

TCP: Bu paket için kullanılan taşıma katmanı protokolünü belirtir.

4434: Bu numara kaynak portun sıra numarasıdır.

80: Hedef port numarası.

[ACK]: Bu, bu bağlamda veri alımının onaylandığını gösteren TCP bayrağıdır.

Seq=23361 Ack=408 Win=6432 Len=4380: Bu ayrıntılar TCP başlık bilgileriyle, sıra ve alındı numaralarını, pencere boyutunu ve paketteki verinin uzunluğunu belirterek ilgilidir.

[Yeniden birleştirilmiş bir PDU'nun TCP bölümü]: Paketin yeniden birleştirilmiş daha büyük bir Protokol Veri Biriminin (PDU) parçası olduğunu belirtir. Bu, bu paketin muhtemelen birden fazla pakete bölünmüş daha büyük bir veri parçasının bir bölümünü taşıdığını öne sürüyor.

Amaç

aldırıları ve kötü amaçlı yazılımları analiz ederek, yürüterek ve tespit ederek IoT cihazlarını korumak

Motivasyon

Topluluğu IoT ekosistemindeki tehditlerden koruyun

Nasıl

Yalnızca kötü amaçlı yazılımları değil aynı zamanda baskınlarını ve açığa çıkan cihazları da çalıştıracak bir laboratuvar oluşturmak ve sürdürmek. Bu, kötü amaçlı yazılımları ve gerçek saldırıları analiz etmemize olanak tanır.

Konferans konuşmaları, makaleler, blog gönderileri, Twitter yayınlarını paylaşma ve IoT güvenliği ile ilgili her türlü soruyu yanıtlama yoluyla sonuçları toplulukla sürekli olarak paylaşmak.

IoT Güvenliğini farklı açılardan ve perspektiflerden ele almak için farklı araştırma çizgilerini takip etmek.

Toplulukla birlikte açık kaynaklı araçlar geliştirmek