Bright Ideas Blog

corelight.blog/2020/12/15/finding-sunburst-backdoor-with-zeek-logs-and-corelight/

Featured Post

May 25, 2022

Corelight Investigator accelerates threat hunting

By Nick Hunter

This morning we announced Corelight Investigator, an open NDR platform that enables security teams with the next-level evidence they need to disrupt attacks and accelerate threat hunting through an easy-to-use, quick-to-deploy SaaS solution. Read more »

Detecting CVE-2022-23270 in PPTP

By Corelight Labs Team – May 26, 2022

This month, Microsoft announced a vulnerability in PPTP, a part of the VPN remote access services on Windows systems that runs on port 1723/tcp. Through Microsoft's MAPP program, Corelight Labs reviewed a proof of concept exploit for this... Read more »

Detecting CVE-2022-26937 with Zeek

By Corelight Labs Team – May 26, 2022

This month, Microsoft announced a vulnerability in NFS. The exploit lies in how an attacker can force a victim NFS server to request an address from the attacker's fake NFS server. The address returned will overflow memory on the victim NFS server... Read more »

Corelight Investigator accelerates threat hunting

By Nick Hunter – May 25, 2022

This morning we announced Corelight Investigator, an open NDR platform that enables security teams with the next-level evidence they need to disrupt attacks and accelerate threat hunting through an easy-to-use, quick-to-deploy SaaS solution. Read more »

Finding CVE-2022-22954 with Zeek

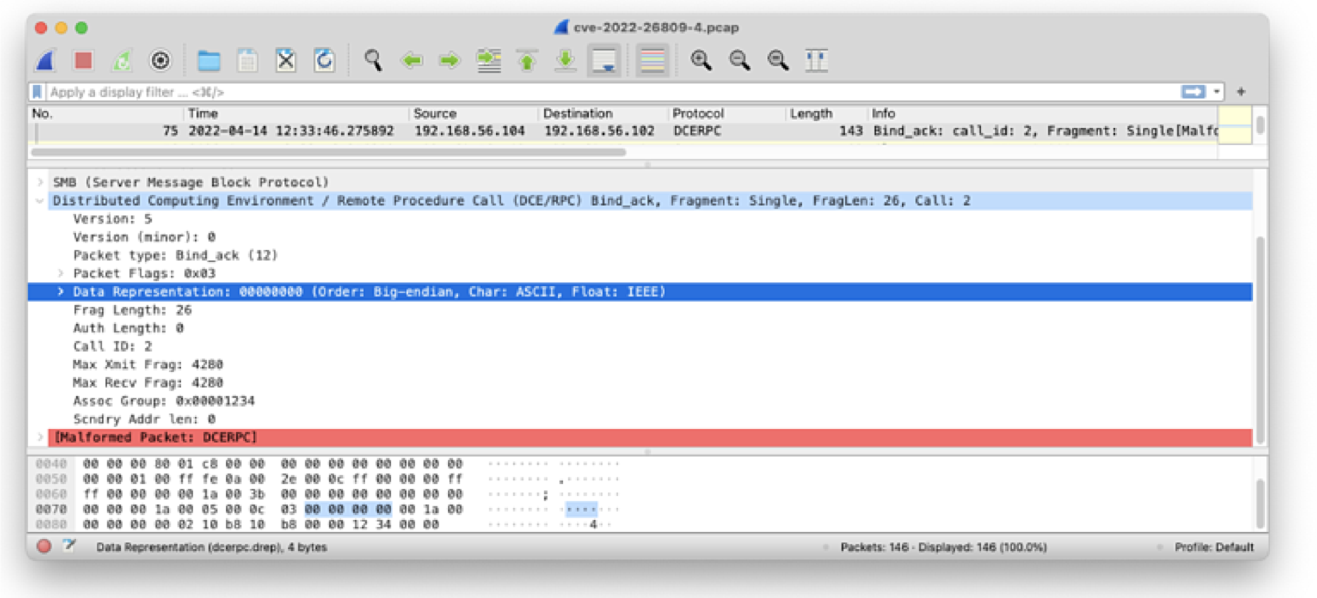
By Corelight Labs Team – May 20, 2022

CISA released a warning to federal agencies on May 18 that APT actors are actively exploiting recent vulnerabilities found in VMware, including CVE-2022-22954. Your first thought may have been to want new signatures, indicators, and/or behavioral... Read more »

What makes evidence uniquely valuable?

By Gregory Bell – May 18, 2022

American novelist F. Scott Fitzgerald famously wrote that "the test of a first-rate intelligence is the ability to hold two opposing ideas in mind at the same time, and still retain the ability to function." All experienced security practitioners... Read more »



```
No.          Time                        Source          Destination     Protocol   Length  Info
          75 2022-04-14 12:33:46.275892  192.168.56.104  192.168.56.102  DCERPC        143  Bind_ack: call_id: 2, Fragment: Single[Malfo
```

```
> SMB (Server Message Block Protocol)
v Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Bind_ack, Fragment: Single, FragLen: 26, Call: 2
    Version: 5
    Version (minor): 0
    Packet type: Bind_ack (12)
  > Packet Flags: 0x03
  > Data Representation: 00000000 (Order: Big-endian, Char: ASCII, Float: IEEE)
    Frag Length: 26
    Auth Length: 0
    Call ID: 2
    Max Xmit Frag: 4280
    Max Recv Frag: 4280
    Assoc Group: 0x00001234
    Scndry Addr len: 0
> [Malformed Packet: DCERPC]
```

```
0040  00 00 00 80 01 c8 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 01 00 ff fe 0a 00  2e 00 0c ff 00 00 00 ff   ........ .,......
0060  ff 00 00 00 00 1a 00 3b  00 00 00 00 00 00 00 00   .......; ........
0070  00 00 00 1a 00 05 00 0c  03 00 00 00 00 00 1a 00   ........ ........
0080  00 00 00 00 02 10 b8 10  b8 00 00 12 34 00 00      ........ ....4..
```

Data Representation (dcerpc.drep), 4 bytes   Packets: 146 · Displayed: 146 (100.0%)   Profile: Default

Another day, another DCE/RPC RCE

By Corelight Labs Team – May 17, 2022

CVE-2022-26809 was patched in Microsoft's previous Patch Tuesday (April 12) and it's a doozy: remote code execution on affected versions of DCE/RPC hosts. The vulnerability attracted a lot of attention in the security community, both because of its... Read more »

Monitoring AWS networks at scale

By Vijit Nair – May 12, 2022

Corelight is pleased to announce our integration with AWS's Traffic Mirroring to Gateway Load Balancer (GWLB) Endpoint as a Target. This integration simplifies the monitoring of network traffic and generating Corelight data in massively scaled-out... Read more »

Spotting Log4j traffic in Kubernetes environments

By Stan Kiefer – May 10, 2022

Editor’s note: This is the latest in a series of posts we have planned over the next several weeks where we explore topics such as network monitoring in Kubernetes, using sidecars to sniff and tunnel traffic, show a real-world example of detecting... Read more »

Network evidence for defensible disclosure

By Richard Bejtlich – May 5, 2022

Editor's note: This is the second in a series of Corelight blog posts focusing on evidence-based security strategy. Catch up on the previous post "Don't trust. verify with evidence." Read more »

Detecting Windows NFS Portmap vulnerabilities

By Corelight Labs Team – April 21, 2022

This month, Microsoft announced two vulnerabilities in portmap, which is part of ONC RPC, on Windows systems. This blog will discuss Zeek detection packages for CVE-2022-24491 and CVE-2022-24497 developed by Corelight Labs. Read more »