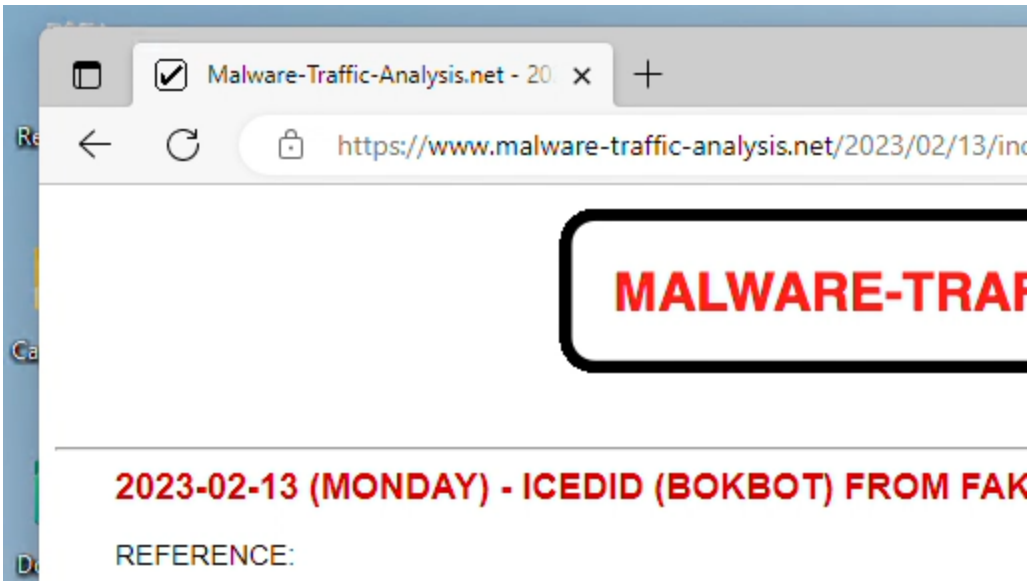
How to Identify IcedID Network Traffic

netresec.com/

February 15, 2023



Erik Hjelmvik

,

Wednesday, 15 February 2023 10:52:00 (UTC/GMT)

Brad Duncan published IcedID (Bokbot) from fake Microsoft Teams page earlier this week. In this video I take a closer look at the PCAP file in that blog post.

> *Note: This video was recorded in a Windows Sandbox to minimize the risk of infecting the host PC in case of accidental execution of a malicious payload from the network traffic.*

As I have previously pointed out, IcedID sends beacons to the C2 server with a 5 minute interval. According to Kai Lu's blog post A Deep Dive Into IcedID Malware: Part 2, this 5 minute interval is caused by a call to WaitForSingleObject with a millisecond timeout parameter of 0x493e0 (300,000), which is exactly 5 minutes.

The IcedID trojan uses a custom BackConnect protocol in order to interact with victim computers through VNC, a file manager or by establishing a reverse shell. There was no IcedID BackConnect traffic in this particular PCAP file though, but several other IcedID

capture files published on malware-traffic-analysis.net do contain IcedID BackConnect traffic. For more information on this proprietary protocol, please see our blog post IcedID BackConnect Protocol.

IOC List

Fake Microsoft Teams download page

- URL: hxxp://microsofteamsus[.]top/en-us/teams/download-app/
- MD5: 5dae65273bf39f866a97684e8b4b1cd3
- SHA256: e365acb47c98a7761ad3012e793b6bcdea83317e9baabf225d51894cc8d9e800
- More info: urlscan.io

IcedID GzipLoader

- Filename: Setup_Win_13-02-2023_16-33-14.exe
- MD5: 7327fb493431fa390203c6003bd0512f
- SHA256: 68fcd0ef08f5710071023f45dfcbbd2f03fe02295156b4cbe711e26b38e21c00
- More info: Triage

IcedID payload disguised as fake gzip file

- URL: hxxp://alishabrindeader[.]com/
- MD5: 8e1e70f15a76c15cc9a5a7f37c283d11
- SHA256: 7eb6e8fdd19fc6b852713c19a879fe5d17e01dc0fec62fa9dec54a6bed1060e7
- More info: IcedID GZIPLOADER Analysis by Binary Defense

IcedID C2 communication

- IP and port: 192.3.76.227:443
- DNS: treylercompandium[.]com
- DNS: qonavlecher[.]com
- X.509 certificate SHA1: b523e3d33e7795de49268ce7744d7414aa37d1db
- X.509 certificate SHA256: f0416cff86ae1ecc1570cccb212f3eb0ac8068bcf9c0e3054883cbf71e0ab2fb
- JA3: a0e9f5d64349fb13191bc781f81f42e1
- JA3S: ec74a5c51106f0419184d0dd08fb05bc
- Beacon interval: 5 minutes
- More info: ThreatFox

Network Forensics Training

Check out our upcoming live network forensics classes for more hands-on network forensic analysis. Our current class material doesn't include any IcedID traffic though, instead you'll get to investigate C2 traffic from Cobalt Strike, TrickBot, njRAT, Meterpreter and a few others.

Posted by Erik Hjelmvik on Wednesday, 15 February 2023 10:52:00 (UTC/GMT)

Tags: #IcedID #CapLoader #Video #Periodicity #a0e9f5d64349fb13191bc781f81f42e1 #ec74a5c51106f0419184d0dd08fb05bc

Recent Posts

» TLS Redirection and Dynamic Decryption Bypass in PolarProxy

» How to Identify IcedID Network Traffic

» CapLoader 1.9.5 Alerts on Malicious Traffic

» Online Network Forensics Class

» IEC-104 File Transfer Extraction

» NetworkMiner 2.8 Released

» NetworkMiner in FLARE VM

» What is a PCAP file?

Blog Archive

» 2023 Blog Posts

» 2022 Blog Posts

» 2021 Blog Posts

» 2020 Blog Posts

» 2019 Blog Posts

» 2018 Blog Posts

» 2017 Blog Posts

» 2016 Blog Posts

» 2015 Blog Posts

» 2014 Blog Posts

» 2013 Blog Posts

» 2012 Blog Posts

» 2011 Blog Posts

List all blog posts

News Feeds

» Google News

» FeedBurner

» RSS Feed

NETRESEC on Mastodon: @netresec@infosec.exchange

NETRESEC on Twitter: @netresec