2020-08-03 -- Qakbot (Qbot) spx147

2020-07-21 -- Emotet infection with Qakbot (Qbot)

2020-07-20 -- Data dump: Emotet with Trickbot

2020-07-20 -- Word docs with macros for IcedID (Bokbot)

2020-07-19 -- Excel doc drops GuLoader

2020-07-17 -- Quick post: Emotet infection

2020-07-16 -- Hancitor infection with info stealer

2020-07-14 -- Pcap and malware for an ISC diary (IcedID)

2020-07-13 -- Dridex infection

2020-07-13 -- Hancitor infection with Ursnif

2020-07-13 -- Word doc drops Hancitor loader

2020-07-10 -- Trickbot gtag chil65 infection

2020-07-09 -- Quick post: Ursnif (Gozi/IFSB) from Italian Word docs

2020-07-09 -- Pcap and malware for an ISC diary (Formbook)

2020-07-07 -- Quick post: Ursnif (Gozi/IFSB) with IcedID from English Word docs

2020-07-01 -- Valak (soft\_sig: mas38) infection with IcedID (Bokbot)

2020-06-30 -- Valak (soft\_sig: mas37) infection with IcedID (Bokbot)

2020-06-29 -- Trickbot version 1000512 and gtag ono51, drops new nwormDll64 module

2020-06-29 -- Two Excel docs that drop Netwire, includes C2 check-ins

2020-06-26 -- Valak (soft\_sig: mad36) infection with IcedID (Bokbot)

2020-06-25 -- Resume-themed malspam pushing ZLoader

2020-06-25 -- Still seeing Trickbot from BLM malspam dated 2020-06-23

2020-06-24 -- Quick post: Valak (soft\_sig: mad35) infection with IcedID (Bokbot)

2020-06-22 -- Quick post: Dridex infection

2020-06-18 -- Qakbot (Qbot) spx143 infection

2020-06-18 -- Password-protected XLS files push ZLoader

2020-06-17 -- Qakbot (Qbot) spx142 infection

2020-06-16 -- Qakbot (Qbot) spx141 infection

2020-06-16 -- Trickbot gtag ono47 infection

2020-06-15 -- Lokibot infection

2020-06-12 -- Qakbot (Qbot) spx139 infection with ZLoader

2020-06-10 -- Ursnif (Gozi/IFSB) infection with Ursnif variant

2020-06-10 -- Quick post: Trickbot gtag gi6 infection in AD environment

2020-06-09 -- Quick post: Valak infection with IcedID (Bokbot)

2020-06-09 -- Pcap and malware for ISC diary (ZLoader)

2020-06-08 -- Quick post: IcedID (Bokbot)

2020-06-08 -- Quick post: Qakbot (Qbot) spx135

2020-06-03 -- Valak (soft\_sig: mad29) infection with IcedID (Bokbot)

2020-06-03 -- Malspam pushing Dridex

2020-06-01 -- Excel doc drops Guloader

2020-06-01 -- IcedID with Image used for Steganography

2020-05-29 -- Quick post: Qakbot (Qbot) spx129 malspam - 82 examples

2020-05-29: Maldoc uses template injection for macro execution

2020-05-27 -- Malspam --> Password-protected zip --> Word doc --> Valak --> IcedID

2020-05-27 -- COVID19-themed Word doc pushes IcedID (Bokbot)

2020-05-26 -- German malspam with password-protected zip files pushes Valak

2020-05-19 -- Pcap and malware for ISC diary (IcedID)

2020-05-15 -- Quick post: 105 examples of German malspam pushing Qakbot spx120

2020-05-14 -- Quick post: FedEx-themed Dridex malspam and infection

2020-05-14 -- Quick post: Qakbot (Qbot) spx119 malspam and infection

2020-05-13: Gamma Ransomware with HTTP check-in

2020-05-13: Cryptbot sample

2020-05-13: Danabot sample with beaconing

2020-05-12 -- Pcap and malware from an ISC diary

2020-05-11 -- Dridex infection from link-based malspam

2020-05-08 -- Quick post: Trickbot (gtag chil13) infection in AD environment

2020-05-07 -- Quick post: Valak infection with IcedID (Bokbot)

2020-05-07 -- Some recent Qakbot (Qbot) stuff

2020-05-05 -- 4 examples of phishing emails with fake login pages

2020-05-04: Trickbot w/ GTAG tt002 and version 1000509, 12 hour PCAP w/ beacons

2020-05-01 -- XLS macro --> Loader EXE --> IcedID (Bokbot)

2020-04-30 -- Password-protected zip files from German malspam push Dridex

2020-04-29 -- Dridex from link-based malspam

2020-04-28 -- Quick post: Dridex malspam and infection

2020-04-27 -- Quick post: Dridex malspam and infection

2020-04-26: Gomorrah stealer (.NET binary)

2020-04-24 -- Quick post: unusual HTTP traffic from Qakbot-infected host

2020-04-23 -- Qakbot (Qbot) spx103 - the "/docs\_[3 characters]/" wave

2020-04-22 -- Qakbot (Qbot) spx102 - the "/pump/" wave

2020-04-21 -- Quick post: Word macro --> Fastloader pushing Trickbot & AnyDesk

2020-04-21 -- Qakbot (Qbot) spx101 - the "/evolving/" wave

2020-04-20 -- Quick post: Trickbot gtag ono38 infection

2020-04-20 -- Qakbot (Qbot) spx100 - the "/vary/" wave

2020-04-17 -- Qakbot (Qbot) spx99

2020-04-16 -- Qakbot (Qbot) spx98

2020-04-16: Trickbot w/ GTAG MAN6 and version 1000507 - Uses revocation.txt config

2020-04-16: AgentTesla data exfil through SMTP

2020-04-15 -- Hancitor malspam and infection traffic

2020-04-14 -- Two infections for GuLoader with NetWire RAT

2020-04-14: Vidar sample with data exfil

2020-04-13: Azorult drops Blackout Ransomware

2020-04-13 -- Quick post: Pcaps for two Trickbot infections

2020-04-13 -- Quick post: Qakbot (Qbot) spx95 infection

2020-04-08 -- Qakbot (Qbot) zip file info

2020-04-07 -- Pcap and malware for an ISC Diary (ZLoader)

2020-04-04: Ave-Maria/Warzon RAT

2020-04-03 -- German and English malspam pushing ZLoader

2020-04-02 -- VBS-based malware infection

2020-03-31 -- material for an ISC diary (Qakbot malspam)

2020-03-31 -- Ursnif (Gozi/IFSB) infection

2020-03-30 -- Invoice-themed malspam pushes Kpot info stealer

2020-03-27 -- price\_request\_9830.doc pushes IcedID (Bokbot)

2020-03-27: Word drops Ursnif through MSHTA.exe

2020-03-26: Word drops Banload banking trojan

2020-03-26: Excel drops AgentTesla

2020-03-26: Word drops IcedId

2020-03-26 -- information\_03\_26.doc pushes ZLoader

2020-03-25 -- Quick post: two pcaps with GuLoader & NetWire RAT infection traffic

2020-03-25: NanoCore sample with dumped plugins (.NET assemblies)

2020-03-24: Blue Botnet

2020-03-23 -- info\_03\_23.doc pushes malware (Valak, maybe?)

2020-03-23 -- Polish malspam with XLS attachment pushes Ursnif (Gozi/IFSB/Dreambot)

2020-03-20 -- IcedID from info\_03\_20.doc

2020-03-19 -- English malspam pushes Ursnif (Gozi/IFSB)

2020-03-19: Formbook

2020-03-18 -- German malspam pushes Ursnif (Gozi/IFSB)

2020-03-17 -- Pcap and malware for an ISC diary (Trickbot as a DLL)

2020-03-16 -- Quick post: malspam known for Ursnif switches to IcedID

2020-03-16 -- More Hancitor malspam using Covid-19/coronavirus theme

2020-03-14: Excel drops LokiBot

2020-03-13 -- Quick post: Qakbot infection

2020-03-12 -- Word doc macro causes a malware infection

2020-03-11 -- Pcap and malware for an ISC diary (Hancitor)

2020-03-10 -- German malspam with password-protected zip files pushing Ursnif

2020-03-09 -- Quick post: Fastloader --> Trickbot gtag wmd44

2020-03-04 -- Quick post: Trickbot spreads from infected client to DC

2020-03-03 -- IcedID (Bokbot) infection

2020-03-03 -- German malspam pushes Ursnif

2020-03-02 -- Quick post: 4 examples of Magnitude EK

2020-02-29: Buer loader

2020-02-26 -- Quick post: Trickbot spreads from infected client to DC

2020-02-25 -- Trickbot gtag red4 distributed as DLL file

2020-02-24 -- Ursnif infection from Italian XLS spreadsheet with macros

2020-02-19 -- Trickbot gtag wecan23 infection

2020-02-18: Remcos

2020-02-13: Turkojan

2020-02-11 -- Pcap and malware for an ISC diary (Ursnif)

2020-02-07 -- Quick post: Emotet epoch 2 infection with Trickbot gtag mor93

2020-02-06 -- Quick post: Pcap of Emotet infection with Trickbot

2020-02-04 -- Pcap and malware for an ISC diary (SocGholish)

2020-01-29 -- Qbot (Qakbot) infection

2020-01-27 -- Pcap and malware for an ISC diary (Emotet with Trickbot)

2020-01-24 -- Italian malpsam pushes Ursnif

2020-01-23 -- German malpsam pushes Ursnif

2020-01-22 -- Quick post: Hancitor infection with Ursnif

2020-01-21 -- Hancitor infection with Cobalt Strike

2020-01-21 -- Pcap and malware for an ISC diary (Ursnif)

2020-01-17 -- Quick post: Emotet epoch 2 infection with Trickbot gtag mor78

2020-01-16 -- Lokibot malspam and infection traffic

2020-01-15 -- Quick post: malspam pushing RevengeRAT

2020-01-14 -- Quick post: Emotet epoch 2 infection with Trickbot gtag mor75

2020-01-10 -- Quick post: IcedID (Bokbot) infection