MY TECHNICAL POSTS - [2013] - [2014] - [2015] - [2016] - [2017] - [2018] - [2019]

- 2019-09-13 -- WSHRAT infection from malspam
- 2019-09-06 -- Qakbot infection from malspam
- 2019-09-05 -- Word doc macro causes Ursnif with Trickbot, or it causes Vidar
- 2019-09-04 -- Data dump: Ursnif doc sends Vidar
- 2019-09-04 -- Data dump: Ursnif infection with Trickbot
- 2019-09-03 -- Pcap and malware for an ISC diary (Remcos RAT)

- 2019-08-31 -- Data dump: Ursnif+Vidar with Trickbot
- 2019-08-27 -- Data dump: Ursnif infection with Trickbot
- 2019-08-26 -- Data dump: SocGholish campaign pushes NetSupport RAT
- 2019-08-23 -- Data dump (Ursnif, Rig EK, Netwire RAT)
- 2019-08-21 -- Ursnif infection with Trickbot
- 2019-08-14 -- Pcap and malware for an ISC diary about MedusaHTTP
- 2019-08-12 -- Data dump: IcedID infection with Trickbot
- 2019-08-02 -- Data dump: two examples of Rig EK
- 2019-08-02 -- Quick post: Lord EK sends Eris Ransomware
- 2019-08-01 -- Newly-discovered Lord Exploit Kit

- 2019-07-29 -- Ursnif infection with Pushdo
- 2019-07-25 -- Hancitor-style Amadey malspam pushes Pony & Cobalt Strike
- 2019-07-22 -- Hancitor switches to Amadey, still pushing Pony/Ursnif/Cobalt Strike
- 2019-07-15 -- Quick post: Recent MyDoom activity
- 2019-07-12 -- Dridex activity
- 2019-07-09 -- Malspam with password-protected Word doc pushes Dridex
- 2019-07-08 -- Quick post: Rig EK sends Amadey
- 2019-07-08 -- Quick post: Ursnif infection with Dridex and Powershell Empire
- 2019-07-05 -- Quick post: Ursnif infection with Trickbot
- 2019-07-03 -- Quick post: Hancitor infection with Cobalt Strike
- 2019-07-02 -- Quick post: Hancitor infection with Cobalt Strike

- Return to main menu
- RSS feed
- @malware_traffic on Twitter

- Traffic analysis exercises
- My technical blog posts
- My non-technical posts
- Guest blog posts

- Tutorials and other entries

- About this blog

- 2019-07-02 -- Quick post: Trickbot Infection with CookiesDll64 module
- 2019-07-01 -- Quick post: Hancitor malspam
- 2019-07-01 -- Quick post: Rig EK sends AZORult

- 2019-06-28 -- Quick post: Fake updates campaign sends Chthonic banking Trojan
- 2019-06-25 -- Quick post: Rig EK sends Pitou.B
- 2019-06-24 -- Pcap and malware for an ISC diary (Rig EK sends Pitou.B)
- 2019-06-18 -- Pcap and malware for an ISC diary (Dridex)
- 2019-06-17 -- Pcap and malware for an ISC diary (Rig EK)
- 2019-06-12 -- Quick post: infection from malware on 80.85.155.70

- 2019-05-23 -- Quick post: malspam pushes Lokibot
- 2019-05-22 -- Rig EK from unknown campaign pushes Gandcrab ransomware
- 2019-05-20 -- Malspam pushes Formbook
- 2019-05-10 -- Quick post: Infection from malspam attachment
- 2019-05-03 -- Quick post: Ursnif infections with Dridex or Nymaim
- 2019-05-01 -- Quick post: Emotet with Trickbot infection traffic
- 2019-05-01 -- Malspam with password-protected Word doc pushes IcedID

- 2019-04-29 -- Quick post: Emotet with Trickbot infection traffic
- 2019-04-27 -- Quick post: Trickbot infection traffic
- 2019-04-24 -- Brazil malspam pushing Banload
- 2019-04-08 -- Quick post: Emotet infection with Qakbot
- 2019-04-05 -- Quick post: Fake Updates campaign pushes Chthonic banking Trojan
- 2019-04-03 -- Quick post: Hookads campaign Rig EK sends AZORult
- 2019-04-02 -- Hancitor malspam with DocuSign theme

- 2019-03-29 -- Quick post: malspam using password-protected word docs pushes Dridex
- 2019-03-20 -- Another example of Spelevo EK
- 2019-03-16 -- Spelevo EK examples
- 2019-03-15 -- Malspam pushes Lokibot
- 2019-03-15 -- Quick post: Change in patterns for Emotet post-infection traffic
- 2019-03-14 -- Quick post: Password-protected Word docs push IcedID (Bokbot)
- 2019-03-13 -- Quick post: Emotet infection with Trickbot
- 2019-03-11 -- Files for an ISC diary (Emotet + Qakbot)
- 2019-03-08 -- Data dump: Emotet malspam and infection traffic
- 2019-03-06 -- Quick post: Korean malspam pushes Flawed Ammyy RAT malware
- 2019-03-04 -- Files for an ISC diary (malspam with password-protected Word docs)

- 2019-03-01 -- Quick post: Emotet infection with Trickbot

- 2019-02-28 -- Fallout EK from the HookAds campaign
- 2019-02-26 -- Quick post: malspam pushing Gandcrab
- 2019-02-22 -- Malspam with Word docs pushing Vidar
- 2019-02-20 -- Quick post: Emotet to IcedID (Bokbot) to Trickbot
- 2019-02-15 -- Quick post: Emotet to IcedID (Bokbot) to Trickbot
- 2019-02-12 -- Quick post: Hancitor infection with Ursnif
- 2019-02-11 -- Pcap and malware for an ISC diary (Fake Updates campaign
- 2019-02-07 -- Info stealer uses FTP to exfiltrate data
- 2019-02-05 -- Pcap for an ISC diary (Hancitor malspam)

- 2019-01-30 -- Data dump (Emotet malspam, Trickbot malspam)
- 2019-01-25 -- Examples from three days of Emotet + follow-up malware
- 2019-01-23 -- Files for an ISC diary
- 2019-01-22 -- Quick post: Emotet + Trickbot, IcedID (Bokbot), or Gootkit
- 2019-01-22 -- Hancitor malspam with FedEx theme
- 2019-01-21 -- Emotet infection with Gootkit
- 2019-01-18 -- Quick post: Emotet infection with IcedID (Bokbot)
- 2019-01-16 -- Hancitor malspam with Paypal theme
- 2019-01-15 -- files for an ISC diary (Emotet infections and follow-up malware)
- 2019-01-14 -- Emotet infection with Gootkit
- 2019-01-11 -- Quick post: Wave of Trickbot malspam (gtag: sat32)
- 2019-01-10 -- HookAds campaign Rig EK pushes Vidar
- 2019-01-10 -- files for an ISC diary ("love you" malspam)
- 2019-01-09 -- Fake AV/tech support scam popup
- 2019-01-04 -- HookAds campaign Rig EK pushes SmokeLoader
- 2019-01-04 -- Malspam pushing Nanocore RAT
- 2019-01-03 -- Malspam pushing Lokibot
- 2019-01-02 -- Malware from malspam pushing Formbook
