OSINT 서비스 툎아보기

2017.07.15

@JG

Open Source INTelligence

intelligence collected from publicly available sources

≠ Open Source Software

≠ Google

OSINT 서비스: FILE/HASH

- HybridAnalysis, https://www.hybrid-analysis.com
- Joe Sandbox, https://www.file-analyzer.net/reports
- Koodous, https://koodous.com
- Malwares.com, https://www.malwares.com
- Malwr, https://malwr.com
- VirusTotal, https://www.virustotal.com

OSINT 서비스: IP

- DomainTools, http://whois.domaintools.com
- DShield, https://www.dshield.org/api
- FireHol IPList, http://iplists.firehol.org
- IPVoid, http://www.ipvoid.com
- Malwares.com, https://www.malwares.com
- Robtex, https://www.robtex.com
- Shodan, https://www.shodan.io
- Whois by KISA, https://whois.kisa.or.kr/kor/whois/openAPI_KeyCre.jsp
- VirusTotal, https://www.virustotal.com

OSINT 서비스: DOMAIN(URL)

- Dshield, https://www.dshield.org/api
- hpHosts, https://hosts-file.net
- Malwares.com, https://www.malwares.com
- Robtex, https://www.robtex.com
- SSL LAB, https://www.ssllabs.com
- URLScan, https://urlscan.io
- URLVoid, http://www.urlvoid.com
- VirusTotal, https://www.virustotal.com

OSINT 서비스: 복합

- Censys, https://www.censys.io
- Cymon, https://cymon.io
- ThreatMiner, https://threatminer.org
- IBM XForce, https://exchange.xforce.ibmcloud.com
- PassiveTotal, https://passivetotal.org
- Maltego, https://www.paterva.com/web7/buy/maltego-clients/maltego.php

Threat Intelligence

Threat = Intent * Capability

Intelligence = Data + Analysis

Data > Infomation > Intelligence

Threat Intelligence 서비스: Freemium

- AlienVault OTX, https://otx.alienvault.com
- ThreatConnect, https://threatconnect.com
- ThreatCrowd, https://threatcrowd.org

Threat Intelligence 서비스: Commercial

- BaeSystem, http://www.baesystems.com/en/product/cyber-technical-services
- CrowdStrike Falcon, https://www.crowdstrike.com
- DigitalShadows, https://www.digitalshadows.com
- FireEye iSight, https://mysight.isightpartners.com
- Group-IB, http://www.group-ib.com/intelligence.html
- IBM Watson, https://www.ibm.com/security/cognitive
- KasperskyLab, https://tip.kaspersky.com
- NSHC RedAlert, http://rais.nshc.net
- Palantir, https://www.palantir.com
- Paloaltonetworks AutoFocus, https://autofocus.paloaltonetworks.com
- RecordedFuture, https://www.recordedfuture.com
- Symantec DeepSight, https://deepsight.symantec.com

Threat Intelligence Life Cycle

Planing/Direction > Collection > Processing > Analysis/Producntion > Disemination

F3EAD: Find > Fix > Finish > Exploit > Analyze > Dissemination

Threat Intelligence 활용: 보안관제

- FEED(IOC) > SIEM || FW || UTM > 탐지 || 차단
- IOC > SIEM > 발견 > 조사

Threat Intelligence 활용: 침해대응

- IP > OSINT > HASH || DOMAIN > 조사
- 조사 > URL > OSINT > HASH > 조사
- HASH > OSINT > HASH

Threat Intelligence 활용: 자동화 & 시각화

- 자동화
  - Automater, http://www.tekdefense.com/automater
  - Cortex, https://github.com/CERT-BDF/Cortex
- 시각화
  - eclectic iq, https://www.eclecticiq.com
  - Palantir, https://www.palantir.com
  - RecordedFuture, https://www.recordedfuture.com

Threat Intelligence 공유: 기술

- STIX, https://stixproject.github.io
- TAXII, https://taxiiproject.github.io
- TLP, https://www.us-cert.gov/tlp

Threat Intelligence 공유: 플랫폼

- Anomali STAXX, ThreatStream, https://www.anomali.com/platform/staxx
- Collective Intelligence Framework, http://csirtgadgets.org
- CRITS, https://crits.github.io
- CTAS, https://cshare.krcert.or.kr:8443
- Cyphon, https://www.cyphon.io
- eclectic iq, https://www.eclecticiq.com
- Facebook Threat eXchange, https://developers.facebook.com/products/threat-exchange
- MISP, http://misp-project.org https://mispppriv.circl.lu
- Soltra, https://soltra.com
- ThreatQ, https://www.threatq.com

Q&A

jnglyu@gmail.com