Network Forensics

Network Forensics

- Involves monitoring and capturing network traffic to identify suspicious behavior such as unauthorized access or data exfiltration.
- Encryption and obfuscation techniques make deep-packet analysis harder.
- **key points**:
  - Packet Capture (PCAP): Monitoring and capturing network packets to analyze communication
  - Log Analysis: Investigating network device logs to reconstruct malicious activity
- **tools**
  - *Wireshark* for packet analysis, *Nmap* for port scanning, X*plico* for application layer analysis, *NetworkMiner* for file extraction, ...

Evidence identification

- **digital footprint and online behavior of individuals or organizations involved in the investigation**
  - n Identifies potential sources of evidence
    - social media profiles, email addresses, domain names, IP addresses, public repositories....
  - locate specific evidences
    - n public accounts related to the suspect or victim, affiliations, ...
  - reveals related accounts, aliases, or associated online identities that may not have been immediately apparent

Evidence collection

- **gather all relevant information without altering it**
- **OSINT may be used as a supplement to digital forensic data**
  - data from publicly available sources
    - archived website snapshots (*Wayback Machine*)
    - online information on registered domains
  - gather digital communications or posts by the suspect on public forums or social media
  - gathers metadata, IP history, or timestamps from online resources, which can support establishing timelines or verifying activities

Data Preservation

- **requirement: all evidence is preserved in its original state, ready for potential court use**
  - screenshots, web archives, metadata retrieval and all publicly available information
    - Adoption of tools that can generate evidence snapshots, including metadata, that allow future verification and defensibility of evidence in court

Analysis

- **support in examining the relationships, patterns, potential evidence connections, timeline reconstruction**
  - reveal connections between individuals, domains, IP addresses, or entities based on shared activities, posts, or affiliations
  - social network analysis, to help identification of assets, third parties involved in the case.
  - trace the origins of digital artifacts
    - emails or messages
    - Identify the sources
    - support analysis of attack vectors and potential leak points
  - origin of digital incidents (through correlation of username, profiles, IPs and known hacker groups)

Report

- **enrich findings to generate a comprehensive report**
  - incorporate attributable public information that helps to reinforce forensic findings
  - incorporates OSINT reports or visualizations to make connections and patterns clearer to readers.
    - e.g. network maps, timelines
  - OSINT sources allow for verification of online evidence, making the final report thorough and defensible.

Network Forensics – OSINT

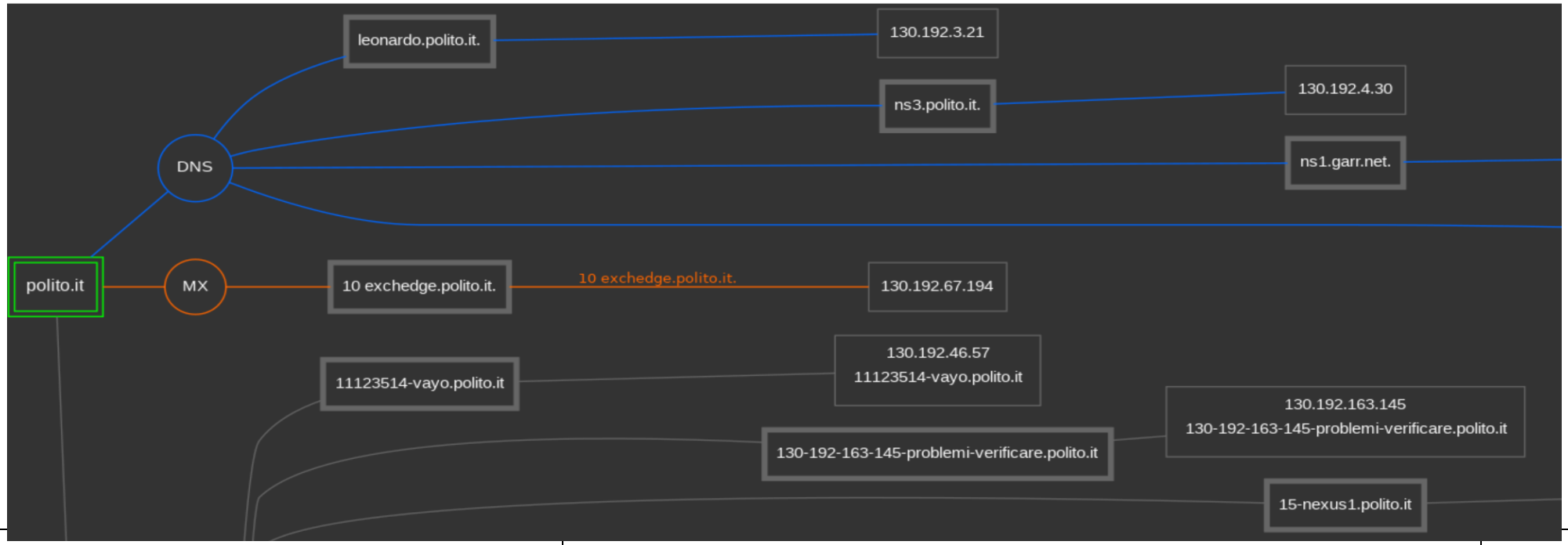
- contextual information about network components
  - Ip addresses
    - Narrow down the geographical location of user/servers
    - e.g.*IPinfo, ip-api.com, MaxMind GeoIP*
    - ip:"8.8.4.4", hostname:"dns.google", anycast:true, city:"Mountain View", region:"California", country:"US", loc:"37.4056,-122.0775", org:"AS15169 Google LLC", postal:"94043", timezone:"America/Los_Angeles",
    - *asn:Object*, asn:"AS15169", name:"Google LLC", domain:"google.com", route:"8.8.4.0/24", type:"hosting",
    - *company:Object*, name:"Google LLC", domain:"google.com", type:"hosting"
    - *privacy:Object*, vpn:false, proxy:false, tor:false, relay:false, hosting:true, service:"",
    - *abuse:Object*, address:"US, CA, Mountain View, 1600 Amphitheatre Parkway, 94043", country:"US", email:"network-abuse@google.com", name:"Abuse", network:"8.8.4.0/24", phone:"+1-650-253-0000",

Network Forensics – OSINT (II)

- Internet service provider and organizational data
  - Whois lookup
    - ownership and assignment details of IP addresses
    - e.g. RIPE NCC *https://apps.db.ripe.net/db-web-ui/query*
      - route: 130.192.0.0/16
      - descr: TORINO-IT-LAN
      - origin: AS137
      - remarks: Politecnico di Torino
      - remarks: Università degli Studi di Torino
      - remarks: To notify abuse mailto: cert@garr.it
      - remarks: Send SPAM complaints to: spam.report@polito.it
      - mnt-by: GARR-LIR
      - created: 2002-04-24T11:36:29Z
      - last-modified: 2024-02-23T15:47:31Z
      - source: RIPE

Network Forensics – OSINT (III)

- domain exploration
  - reverse DNS lookups to identify domains associated with IP
  - can reveal related websites, services, subdomains (… and possible different purposes)
  - e.g. *DNSDumpster, Shodan*



Network Forensics – OSINT (IV)

- service detection
  - open ports and running services
    - e.g. *Nmap*
  - Databases of scanned IPs, revealing device type, versions, configurations
    - e.g. *Censys, Shodan, spiderfoot*

Network Forensics – OSINT (V)

- Mentions
  - IP addresses and network object In social media, paste sites
    - As part of security alerts and incidents
  - e.g. *Pastebin, TweetDeck ((obsolete)*
    - *site:pastebin.com "polimi.it"*
    - *site:pastebin.com "password" "polimi.it"*

Network Forensics – OSINT (VI)

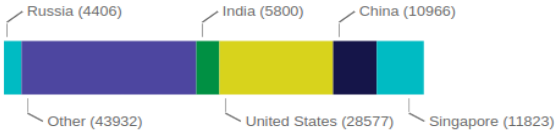
- Threat intelligence feed
  - threat intelligence databases often mark suspicious IPs linked to malicious activity
    - e.g. *virusTotal, alienvault OTX, ...*

MALWARE FAMILIES: #LowFi:BRUTE:Win32/Iminent, SSH Brute-Force

ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

Indicators of Compromise (171K) | Related Pulses (0) | Comments (2) | History (3)

TYPES OF INDICATORS



THREAT INFRASTRUCTURE

Show 10 entries

TYPE	INDICATOR	ROLE	TITLE	ADDED
IPv4	122.191.109.66	bruteforce	SSH intrusion attempt from 122.191.109.66	Aug 11, 2024, 12:30:23 AM
IPv4	47.236.232.63	bruteforce	SSH intrusion attempt from 47.236.232.63	Aug 11, 2024, 1:05:59 AM
IPv4	1.13.181.190	bruteforce	SSH intrusion attempt from 1.13.181.190	Aug 11, 2024, 1:07:16 AM
IPv4	165.154.11.113	bruteforce	SSH intrusion attempt from 165.154.11.113	Aug 11, 2024, 1:16:23 AM
IPv4	190.183.61.91	bruteforce	SSH intrusion attempt from 190.183.61.91	Aug 11, 2024, 1:27:17 AM

Network Forensics – OSINT (VII)

- IP history
  - Previous association with different (suspicious) domains
  - e.g. *viewDNS.info, RiskIQ*

DNS Report for polito.it
==========

Parent Nameserver Tests

Status	Test Case	Information
i	NS records listed at parent servers	Nameserver records returned by the parent servers are: giove.polito.it. [130.192.3.24] [TTL=3600] ns1.garr.net. [NO GLUE] [TTL=3600] ns3.polito.it. [130.192.4.30] [TTL=3600] leonardo.polito.it. [130.192.3.21] [TTL=3600] This information was kindly provided by a.dns.it.
✓	Domain listed at parent servers	Good! The parent servers have information on your domain. Some other domains (like .co.us) do not have a DNS zone at the parent servers.
✓	NS records listed at parent servers	Good! The parent servers have your NS records listed. If they didn't, people wouldn't be able to find your domain!
✓	Parent servers return glue	Good! The TLD of your domain (it) matches the TLD of your nameservers (it) and hence the parent servers MUST return the IP (glue) for your NS records... AND THEY DO!
⚠	A record for each NS at parent	Oops! The parent servers don't have A records for each of your nameservers! This isn't a fatal error but means an extra lookup needs to be performed increasing the load time to your site.

Social Media Forensics

- **analysis of social media accounts and activities**
  - gathering information from public profiles, posts, and metadata
  - extract data from social media accounts
    - Behavior and timing of activities
    - identify associations (e.g. linked accounts)

Social Media Forensics (III)

- **User Profiling and Attribution**
  - accounts cross-correlation
  - online activity metadata analysis
  - network graphing of interaction
    - e.g. *Maltego, spiderfoot*
- **Geospatial analysis**
  - analysis of embedded data location (GPS, Exif data)
    - exiftool
  - reverse image search

Social Media Forensics (II)

- **Relationships**
  - follower/following allow for identification of mutual friends
  - Comments shows recurring interactions
- **Content analysis**
  - trend and topics
  - user emotional state and motivation
- **Image and Video analysis**
  - reverse search (origin verification)
  - facial recognition

Social Media Forensics (III)

- **monitoring of relevant activity**
  - Hashtags, keyword
- **detection of fake information**
  - puppet profiles
    - analysis of fake activity
  - impersonating users
    - behavioral similarities across different profiles