Network Analysis Report – Malware Compromise

Platform: BlueTeamLabs

Lab: OnlineNetwork Analysis: Malware Compromise

Evidence: traffic-with-drideix-infection.pcap

Summary

A PCAP was analyzed after a SIEM alert indicated communication with a known malicious domain from an internal user workstation (Sara, Accountant). The user reported opening an “invoice” document containing a macro and the program crashed.

Network evidence shows a clear infection chain: malicious DNS resolution, HTTP download of a Windows PE payload disguised with a non-exe extension, additional staged file download (RAR), and subsequent beacon/C2-like activity. Zui/Suricata alerts further support Ursnif/Dridex-related network patterns, including a malicious SSL certificate blacklist hit and Ursnif C2 beacon signatures.

Compromised host: 10.11.27.101

Primary malicious infrastructure: klychenogg.com → 95.181.198.231

Scope and PCAP Overview

- **First packet time:** 2018-11-27 11:30:12
- **Last packet time:** 2018-11-27 12:12:16
- **Total duration:** 00:42:03
- **Total packets:** 2053

Protocol Overview (Wireshark)

Traffic is primarily TCP with smaller amounts of TLS, HTTP, and DNS. This aligns with typical malware behavior: DNS resolution → payload delivery via HTTP → follow-on communications over HTTP/TLS.

Wireshark · Protocol Hierarchy Statistics · traffic-with-dridex-infection.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	2053	100.0	1178802	3,737	0	0	0	2053
Ethernet	100.0	2053	2.4	28742	91	0	0	0	2053
Internet Protocol Version 4	100.0	2053	3.5	41060	130	0	0	0	2053
User Datagram Protocol	0.8	17	0.0	136	0	0	0	0	17
Domain Name System	0.8	17	0.1	1253	3	17	1253	3	17
Transmission Control Protocol	99.2	2036	3.5	41536	131	1706	34936	110	2036
Transport Layer Security	15.5	318	14.4	169625	537	318	169625	537	318
Hypertext Transfer Protocol	0.6	12	22.4	264140	837	6	2146	6	12
Media Type	0.1	2	22.0	259449	822	2	259449	822	2
Line-based text data	0.1	3	41.6	489960	1,553	3	489960	1,553	3
Data	0.0	1	22.2	261120	827	1	261120	827	1

Tools

Tools Used

- Wireshark: protocol hierarchy, conversations, filters, Follow HTTP/TCP Stream
- Zui (Brimdata): review Suricata/Zeek outputs and alert events using queries
- VirusTotal: reputation checks for domains, IPs, and file hashes

Findings and Evidence

1. Victim Host Identification

Wireshark conversations show consistent outbound activity from 10.11.27.101, including DNS lookups, HTTP downloads, and TLS sessions. This host is assessed as the infected workstation.

Victim: 10.11.27.101

Ethernet · 1 | IPv4 · 9 | IPv6 | TCP · 51 | UDP · 8

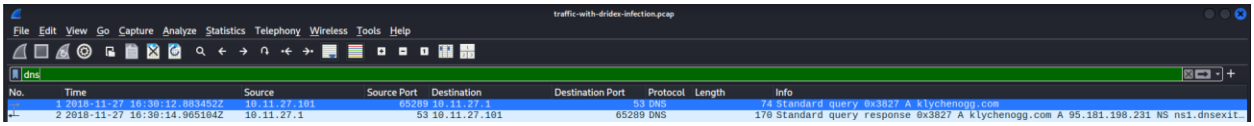
Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.11.27.101	95.181.198.231	558	546 kB	1	152	9 kB	406	538 kB	2.123144	537.1739	130 bits/s	8,008 bits/s
10.11.27.101	176.32.33.108	458	405 kB	2	156	10 kB	302	395 kB	24.283321	5.8906	13 kbps	536 kbps
10.11.27.101	83.166.247.211	711	117 kB	4	378	53 kB	333	64 kB	99.256729	2424.2444	174 bits/s	212 bits/s
10.11.27.101	172.106.33.46	79	28 kB	6	40	21 kB	39	7 kB	698.722003	1457.7267	113 bits/s	37 bits/s
10.11.27.101	185.158.251.55	77	27 kB	7	39	21 kB	38	7 kB	838.328764	1464.5101	112 bits/s	36 bits/s
10.11.27.101	185.244.150.230	76	27 kB	5	39	21 kB	37	7 kB	524.881874	1466.4519	112 bits/s	35 bits/s
10.11.27.101	174.34.253.11	77	27 kB	8	39	20 kB	38	6 kB	990.749952	1447.6811	111 bits/s	34 bits/s
10.11.27.101	10.11.27.1	11	1 kB	0	5	377 bytes	6	1 kB	0.000000	2118.5054	1 bits/s	3 bits/s
10.11.27.101	208.67.222.222	6	575 bytes	3	3	239 bytes	3	336 bytes	96.715429	0.1224	15 kbps	21 kbps

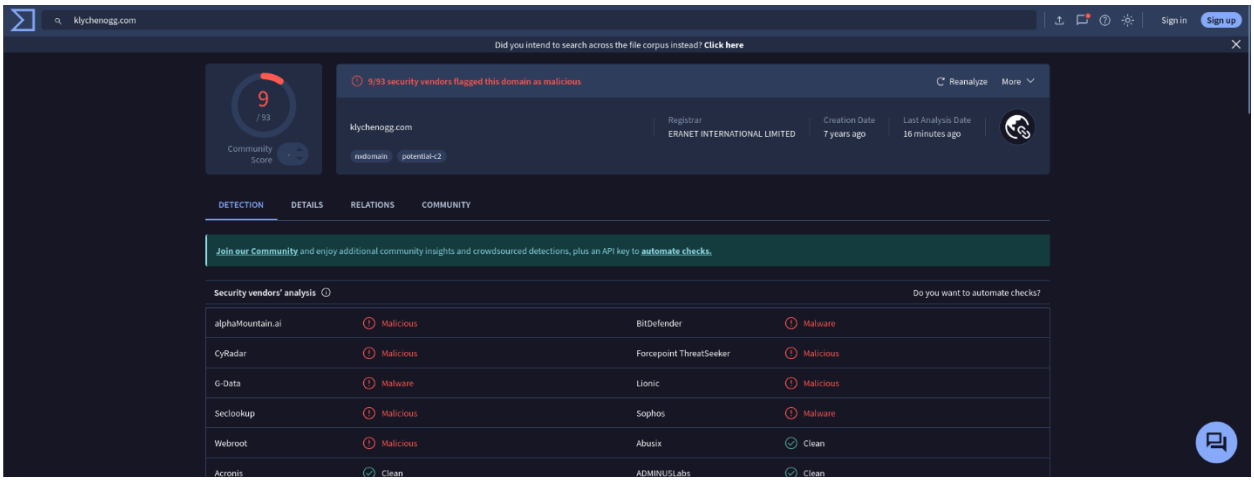
2. Malicious DNS Resolution

A DNS query was observed for a suspicious domain which resolved to an external IP address:

- **Domain queried:** klychenogg.com
- **Resolved A record:** 95.181.198.231
- **VirusTotal:** domain flagged as malicious (9 vendors observed)

This is an early indicator of compromise and likely points to malware staging or command-and-control infrastructure.





3. HTTP Download of Disguised Windows Executable (PE)

Following DNS resolution, the victim downloaded content from the resolved IP using HTTP. The payload was delivered using a non-exe extension, but the content begins with the Windows PE header (“MZ”), confirming an executable.

HTTP Request

- Source: 10.11.27.101
- Destination: 95.181.198.231:80
- Request: GET /QIC/tewokl.php?l=spet10.spr HTTP/1.1
- Host: klychenogg.com

HTTP Response Indicators

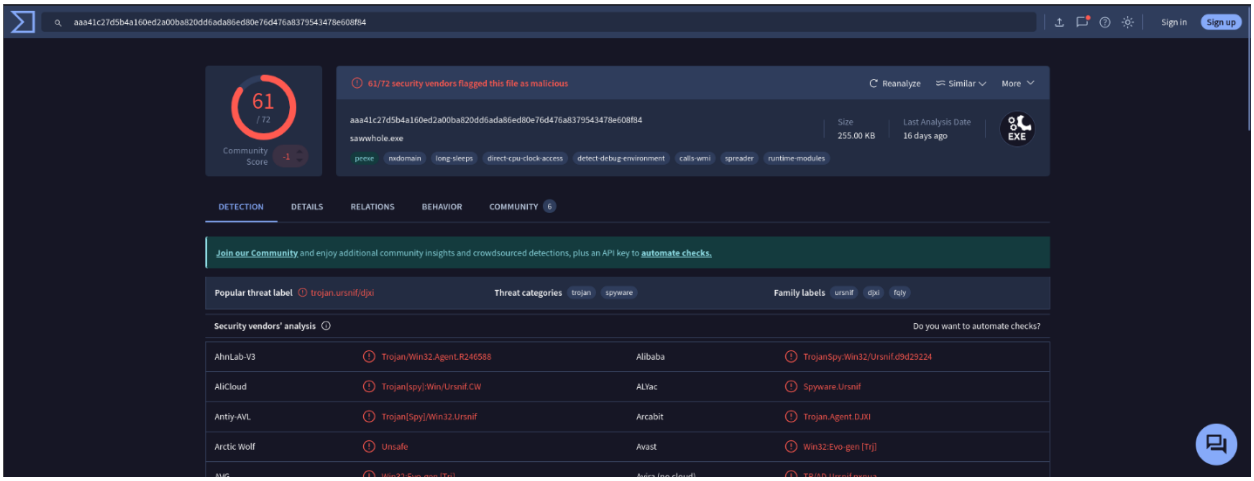
- HTTP/1.1 200 OK
- Content-Type: application/octet-stream
- Response body begins with: MZ ... This program cannot be run in DOS mode.

This behavior is consistent with macro/downloader malware delivering a PE payload via HTTP while disguising the filename/extension.

Extracted File Hashes (Payload)

- **MD5:** 961d559e9aaa58534cc8331a1f8094ae
- **SHA-1:** 946b241758216ed34793de0512c54efa0d629918
- **SHA-256:** aaa41c27d5b4a160ed2a00ba820dd6ada86ed80e76d476a8379543478e608f84

VirusTotal: SHA-256 flagged as malicious by 61/72 vendors (observed) and labeled with trojan/ursnif/drixi family associations.



4. Additional Stage Download (RAR)

A second suspicious file download was observed from the same infrastructure:

- Source: 10.11.27.101
- Destination: 95.181.198.231:80
- Request: GET /oiioiashdqbwe.rar HTTP/1.1
- Response: HTTP/1.1 200 OK
- Content-Type: application/rar

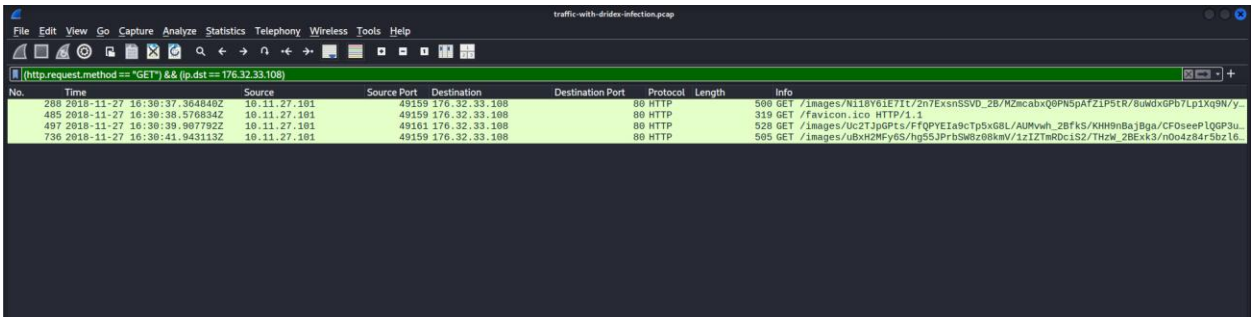
This suggests a staged download process (additional components/tools packaged in a RAR).

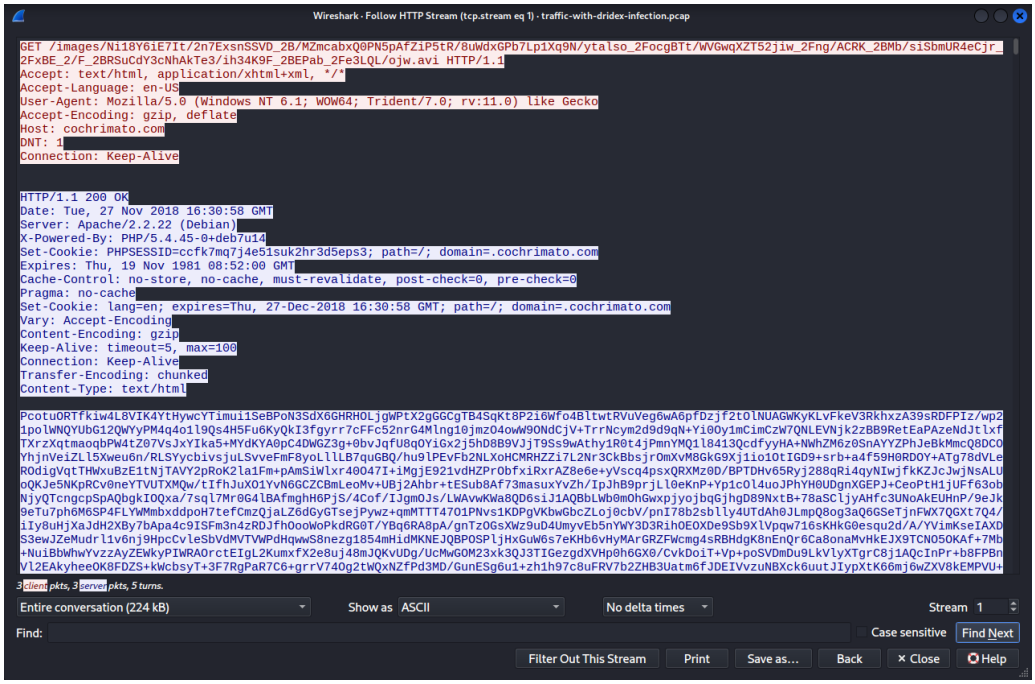
5. Suspicious HTTP Requests to Another Host (Flagged Domain)

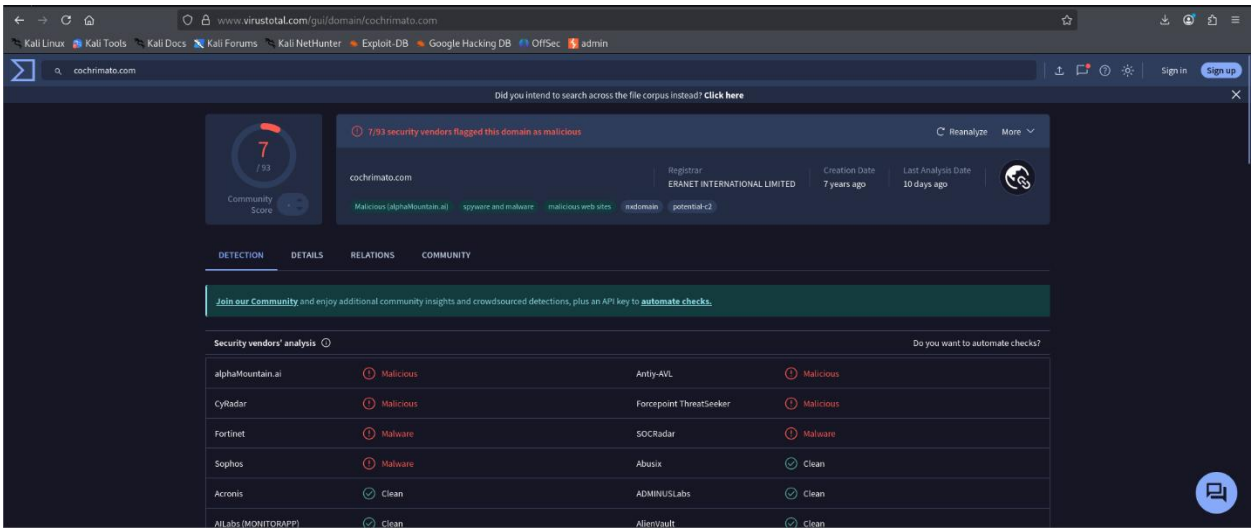
Filtering HTTP GET requests to destination 176.32.33.108 revealed multiple requests where the Host header was:

- Host: cochrimato.com
- VirusTotal: domain flagged as malicious (7 detections observed)

This indicates additional suspicious web activity potentially related to the infection chain (staging, redirects, tracking, or secondary infrastructure).





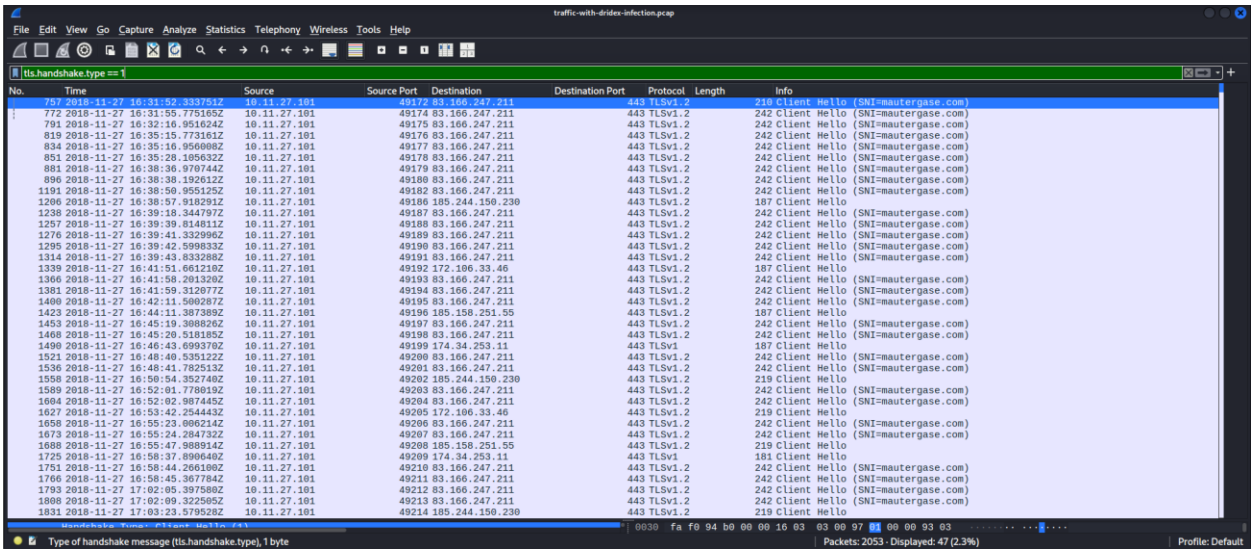


6. **TLS Handshakes with SNI mautergase.com**

Using the filter tls.handshake.type == 1, multiple TLS ClientHello messages were observed. The Info column shows repeated:

- Client Hello (SNI = mautergase.com)

SNI (Server Name Indication) is valuable in TLS 1.2 traffic because it reveals the hostname the client attempted to reach even when traffic content is encrypted. The repeated ClientHello events are consistent with beaconing/retry behavior commonly seen in malware C2 communications.



Zui / Suricata Alert Analysis

Zui was used to review IDS alerts generated from the PCAP. Alerts were filtered using:

event_type=="alert"

Key Alert Signatures Observed

1. **ET MALWARE Likely Evil EXE download from MSXMLHTTP non-exe extension M2**

   This supports the finding that the victim downloaded a Windows executable disguised as a non-exe file via HTTP (common in macro + MSXMLHTTP download behavior).

2. **ET POLICY PE EXE or DLL Windows file download HTTP**

   This indicates a PE file transfer over HTTP (often informational but confirms the presence of executable downloads).

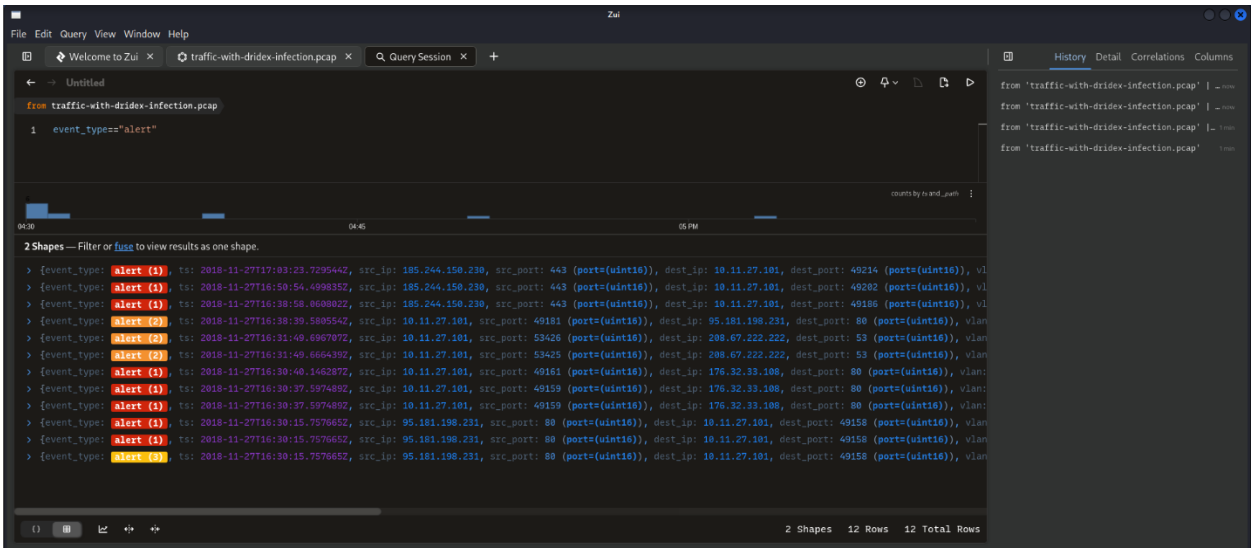
3. **ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)**

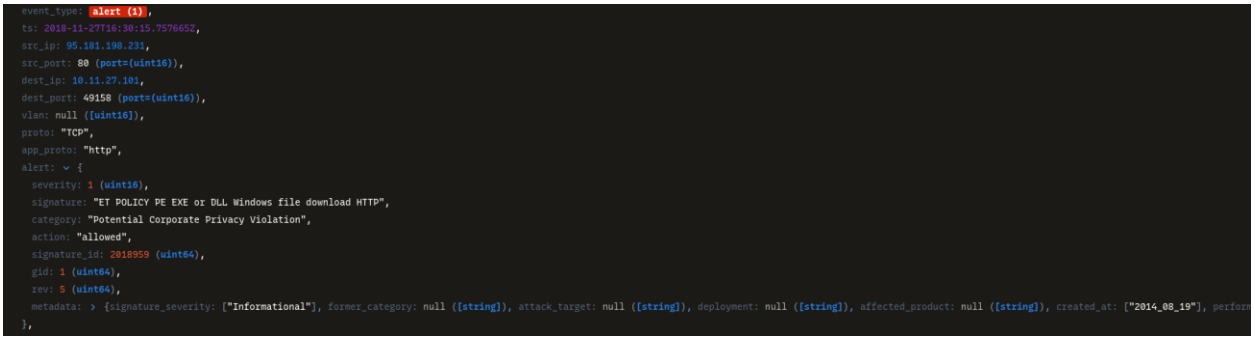
   This indicates HTTP request patterns consistent with Ursnif-style command-and-control beaconing.

4. **ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)**

   High-signal TLS detection: indicates the TLS certificate matched a known malicious fingerprint associated with Dridex ecosystem indicators.

Alert details also showed action: allowed, meaning the traffic was not blocked.





High-Level Timeline

1. Victim host 10.11.27.101 performs DNS lookup for klychenogg.com → resolves to 95.181.198.231.
2. Victim downloads an executable payload over HTTP from klychenogg.com using a disguised extension (spet10.spr) through tewokl.php.
3. Victim downloads a RAR archive (/oiioiashdqbwe.rar) from the same host.
4. Victim generates additional HTTP GET requests involving host cochrimato.com (destination 176.32.33.108).
5. Victim exhibits TLS C2-like activity, repeatedly attempting TLS sessions with SNI mautergase.com, and Suricata flags Dridex-related SSL blacklist indicators.

MITRE ATT&CK Mapping (Network-Observable)

T1566.001 – Phishing: Spearphishing Attachment (scenario context: macro invoice)

T1204.002 – User Execution: Malicious File (user opened macro doc)

T1105 – Ingress Tool Transfer (payload download over HTTP, RAR stage)

T1071.001 – Application Layer Protocol: Web Protocols (HTTP-based C2 patterns)

T1573 – Encrypted Channel (TLS communications; SNI observed)

T1568 – Dynamic Resolution (DNS resolution of malicious domains)

Conclusion

The PCAP contains strong evidence of a macro-driven malware compromise with staged payload delivery and command-and-control activity. Malicious DNS resolution led to HTTP downloads of a disguised Windows executable and a secondary RAR archive. Subsequent suspicious HTTP activity and repeated TLS ClientHello messages with SNI mautergase.com, combined with Suricata alerts (Ursnif beacon + Dridex SSL blacklist), support the conclusion that the host 10.11.27.101 was compromised and communicated with malicious infrastructure.