

Network Analysis Report – Malware Compromise

Platform: BlueTeamLabs

Lab: OnlineNetwork Analysis: Malware Compromise

Evidence: traffic-with-druidex-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.

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

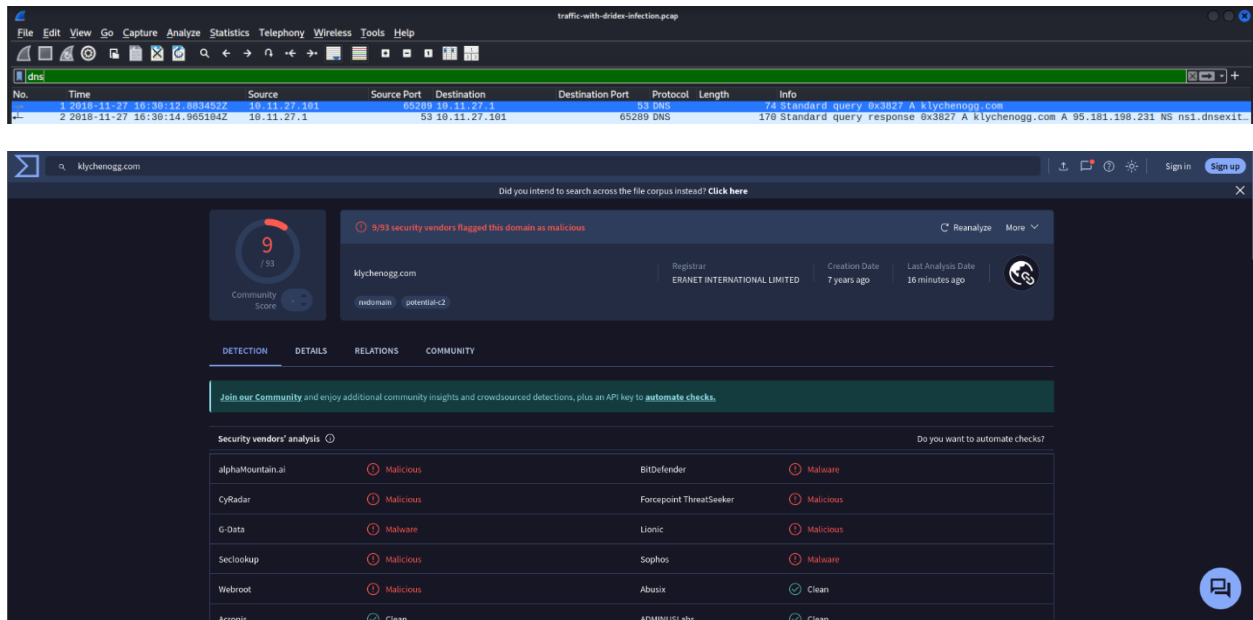
Ethernet - 1	IPv4 - 9	IPv6	TCP - 51	UDP - 8	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.11.27.101	95.181.198.231		558	546 kB	1	152	9 kB	406	538 kB	2.123144	537.1739	130 bits/s	8,008 kbps
10.11.27.101	176.32.33.108		458	405 kB	2	156	10 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.

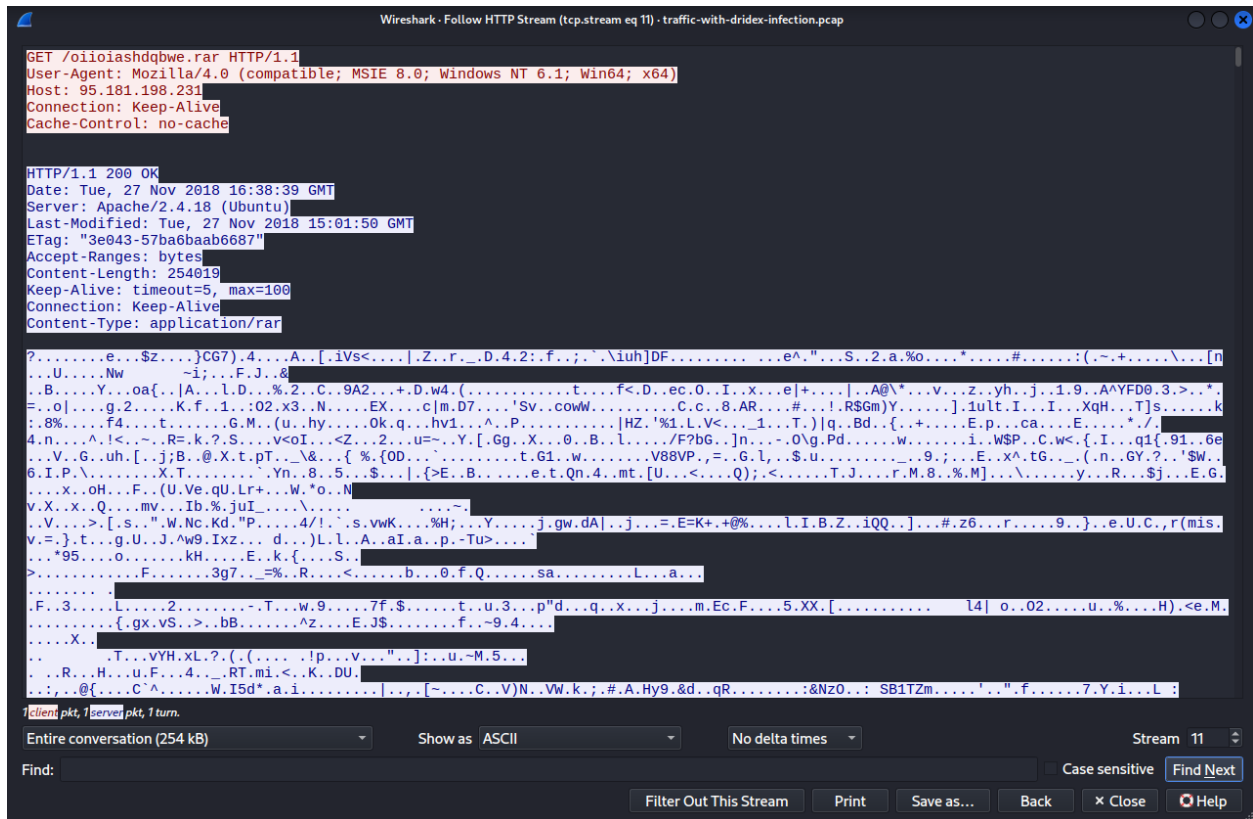
This behavior is consistent with macro/downloader malware delivering a PE payload via HTTP while disguising the filename/extension.

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).

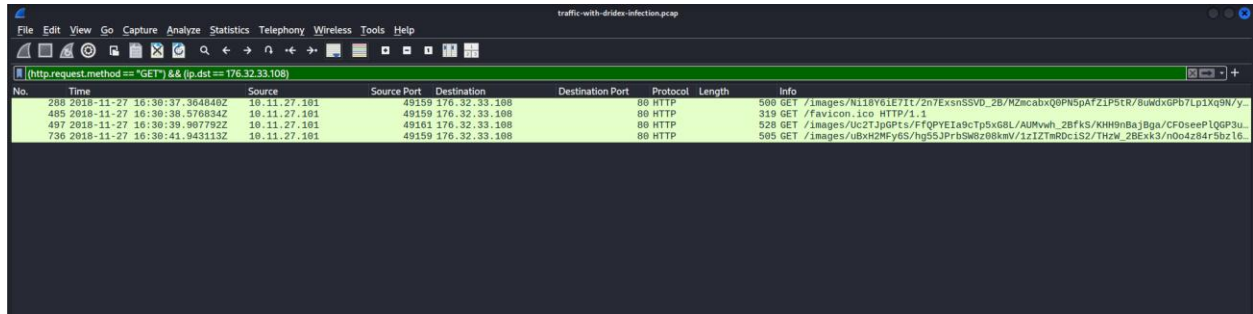


5. Suspicious HTTP Requests to Another Host (Flagged Domain)

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

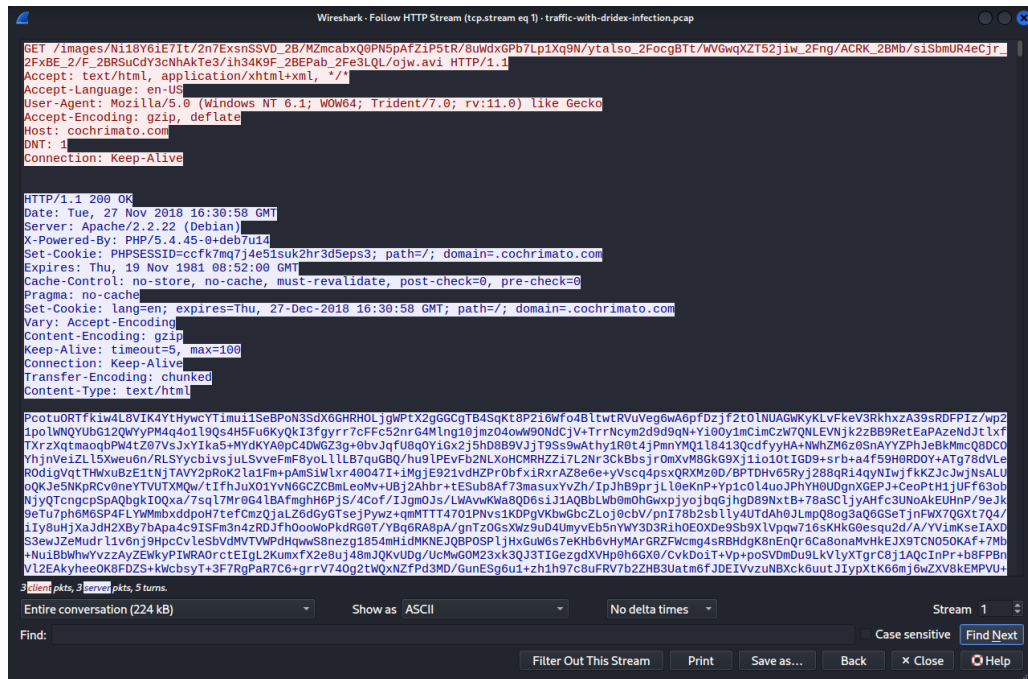
- Host: cochrimato.com
- VirusTotal: domain flagged as malicious (7 detections observed)

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



Wireshark packet capture showing HTTP traffic. The packet list displays four packets (288, 485, 497, 736) all of type GET, originating from 10.11.27.101 and destined for 49.159.176.32.33.108. The packet details pane shows the raw data of the first packet, which is a GET request for /images/1118Y61E7I/2n7ExnsSSVD_2B/MZmcabxQ0PN5pAfZ1P5tR/8uWdxGPb7Lp1Xq9N/ytalso_2FocgBtT/WGwqXT52jiw_2Fng/ACRK_2Bmb/s1SbmUR4eCjR_2FxBE_2/F_2BR5ucdy3cNhakTe3/iH34K0F_2BEPab_2Fe3LQL/0jw.avi HTTP/1.1.

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
288	2018-11-27 16:30:37.3648402	10.11.27.101	49159	176.32.33.108	80	HTTP	500	GET /images/1118Y61E7I/2n7ExnsSSVD_2B/MZmcabxQ0PN5pAfZ1P5tR/8uWdxGPb7Lp1Xq9N/y...
485	2018-11-27 16:30:38.5706342	10.11.27.101	49159	176.32.33.108	80	HTTP	319	GET /favicon.ico HTTP/1.1
497	2018-11-27 16:30:39.9077922	10.11.27.101	49101	176.32.33.108	80	HTTP	528	GET /images/uc2T3pGPts/FTQPYEia9cTp5xGBL/AUMvwh_2BFks/KHH9nBaJBga/CF0seepLQGP3u...
736	2018-11-27 16:30:41.9431132	10.11.27.101	49159	176.32.33.108	80	HTTP	505	GET /images/uBxH2MFy6S/hg55JPrb5W6z8kmV/1z1ZTmR0c1S2/ThzW_2BEkx3/n0o4z84r5bz16...



Wireshark - Follow HTTP Stream (tcp.stream eq 1) - traffic-with-drindex-infection.pcap

GET /images/1118Y61E7I/2n7ExnsSSVD_2B/MZmcabxQ0PN5pAfZ1P5tR/8uWdxGPb7Lp1Xq9N/ytalso_2FocgBtT/WGwqXT52jiw_2Fng/ACRK_2Bmb/s1SbmUR4eCjR_2FxBE_2/F_2BR5ucdy3cNhakTe3/iH34K0F_2BEPab_2Fe3LQL/0jw.avi HTTP/1.1

Accept: text/html, application/xhtml+xml, */*

Accept-Language: en-US

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Accept-Encoding: gzip, deflate

Host: cochrimoto.com

Cookie: PHPSESSID=ccfk7mq74e5isuk2hr3d5eps3; path=/; domain=cochrimoto.com

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: lang=en; expires=Thu, 27-Dec-2018 16:30:58 GMT; path=/; domain=cochrimoto.com

Vary: Accept-Encoding

Content-Encoding: gzip

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Transfer-Encoding: chunked

Content-Type: text/html

HTTP/1.1 200 OK

Date: Tue, 27 Nov 2018 16:30:58 GMT

Server: Apache/2.2.22 (Debian)

X-Powered-By: PHP/5.4.45-94deb7u1

Set-Cookie: PHPSESSID=ccfk7mq74e5isuk2hr3d5eps3; path=/; domain=cochrimoto.com

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: lang=en; expires=Thu, 27-Dec-2018 16:30:58 GMT; path=/; domain=cochrimoto.com

Vary: Accept-Encoding

Content-Encoding: gzip

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Transfer-Encoding: chunked

Content-Type: text/html

PcotuORTfkiw4L8VIK4YthYwYtImu11SeBPon3SdX6GHRH0LjgWPTX2gG6GtB4SqKt8P2i6Wf04B1twtrVuVeg6wA6pfDzjf2t0lNUAGWkyKLVfKev3RkhxzA39sRDEPIZ/wp2

lpo1wNQYU6G12QwYpYp440119Q64H5F-u8kyQK13fyrr77FFc52nrG4M1ng10jnz204ow90N0CjVvTrNcyzn20d99N+Yi00ymCmC2w7QNLVnjK2z889ReEaPazend3tLxf

TXrZxqtmaoqPM4tZ67VsJxYIka5MYdKYA0pC4DMGZ3g+0bvJqF8qY16x2j5h08B9VjJT9S9wAthy1R8t4jPmYMQ118413qcdfyYHA+NwhZM6z0SnAYYZPhJebKmmCQ8DC0

YhjnVeZL15Xweu6n/RLSYcbivjsuLSvveFmFBoYL11B7quGBQ/hu9lPEVfB2NLXoHMRHZ17L2Nr3ckBbsjromXvM8GK9Xj11o10tIG09+srB+a4f59H8RD0Y+AtG78dVLe

R0D1qVqtTmWxubZEt1NjTAYVZpR0K21a1Fm+pAmSiWlXr40047I+IMgJE921vdHZP0bfx1RrAZ8e6e+yVscq4psxQRXmZ0D/BPTDHv65RyJ288qR14qyN1wjfKZJc3JwJNsALU

oKJJe5mKpR0vneTVUUXMQw/t1fhJux01YvNGGZCBMLeomV+UBj2Ahr+tESub8Af73masuxYvZh/IpJhB9prjLl0eKnP+Yp1c0L4uoJPHYH0UDgnXGEpJ+CeoPth1jUFf630b

NjyQTcngcpSpAqBgk10Qxa/7sq17Mr0G41BAfmghH6PjS/4Cof/I3gm03s/LWAvwKwa8QD6s1J1AQ8BlWb0m0hGwXpJyojbqGjhgD89NxtB+78aSClJyAhfC3UNoAkeUHNp/9eJk

9e7U7ph6MSP4FLVWmbxdp0h7teFcmZQjALZ6d6y6TsejPywz+qeMTT4701PNvsiKDPgVkbWGbCZLoj0cbv/pnI78D2sb1ly4UtdAh0JLmpQ8og3aQ6G6seTjnfW7Q6xt7Q4/

11y8uHjXaJdX2B7bApa4e91Sf3m342R0Jfh0o0wPkdR0T/YBq6R8pA/gntZ0GxW29dU4myvEb5nYw3D3R2h0EOXD0eS9b9XVp9w716XKH0besquZd/A/YVimKseIAXD

S36wJZEMudr11v6nj9HpcCyLeSbvdMTWpDhQwS8nezg1854Mh1dMKNEJQBPOSP1jHGuW6s7ekHb6vHyMarGRZFWcmg4sRBHdgK8EnQr6ca8onAhVhKEJX9TCN050KAf+7Mb

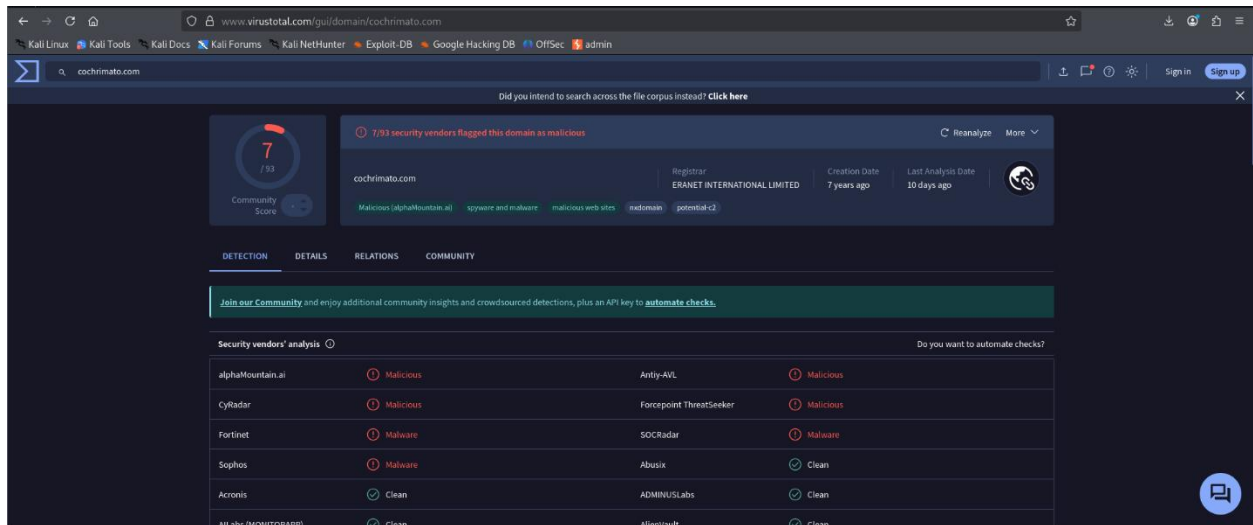
+Nu1BbhwvYzayZEWkyPIwR0rctEiGL2KumFX2eBuJ48mJQKVUDG/UcMwGOM23xk3QJ3TI6ezdXVH0h6GX8/CvkD01+Vp+posVDmbDu9LkVlyXtgrC8j1A0cInPr+8BFPB

VL2EakyheeOK8FD2S+3F7RgPaR7C6+grrV740g2tWqXNZfPd3MD/GunEsg6u1+zh1h97c8uFRV7b2ZHB3Uatm6fJDEIVvzUNBXck6uutJ1ypXtK66mj6wZxV8KEMPVU+

3 client pkts, 3 server pkts, 5 turns.

Entire conversation (224 kb) Show as ASCII No delta times Stream 1

Find: Filter Out This Stream Print Save as... Back X Close Help



VirusTotal scan results for cochrimoto.com. The domain is flagged as malicious by 7/93 security vendors. The analysis shows various security vendors' results, including Malicious (alphaMountain.ai), Malware (CyRadAr, Fortinet, Sophos), and Clean (Acronis, Ali Labs).

Did you intend to search across the file corpus instead? [Click here](#)

7/93 security vendors flagged this domain as malicious

Reanalyze More

cochrimoto.com

Registrar: ERANET INTERNATIONAL LIMITED

Creation Date: 7 years ago

Last Analysis Date: 10 days ago

Malicious (alphaMountain.ai) spyware and malware malicious web sites redomain potential C2

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

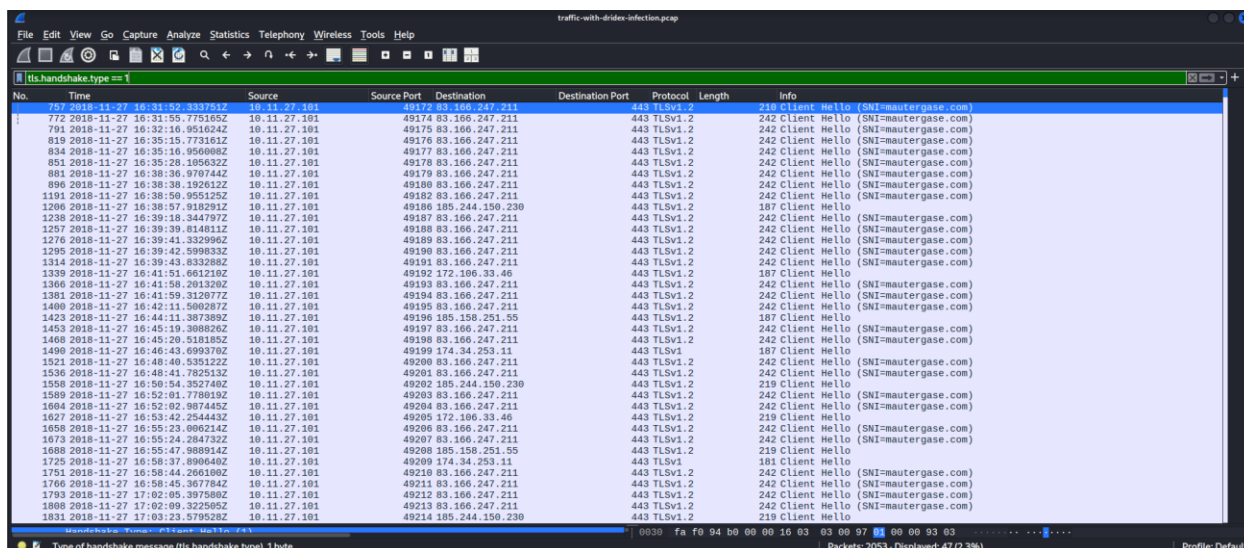
Vendor	Result
alphaMountain.ai	Malicious
CyRadAr	Malicious
Fortinet	Malware
Sophos	Malware
Acronis	Clean
Ali Labs (MONITORAPP)	Clean
Antiy-AVL	Malicious
Forcepoint ThreatSeeker	Malicious
SOCradar	Malware
Abusix	Clean
ADMINUS Labs	Clean
AlienVault	Clean

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.



The image shows a Wireshark packet capture of network traffic. The filter bar at the top is set to `tls.handshake.type == 1`. The packet list on the left shows a series of ClientHello messages (type 1) from various source IP addresses to destination IP 83.166.247.211. The packet details pane on the right shows the structure of a TLS ClientHello message, including the SNI field which contains `mautergase.com`. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
767	2018-11-27 16:31:52.333761Z	10.11.27.101	49172	83.166.247.211	443	TLSv1.2	216	Client Hello (SNI=mautergase.com)
772	2018-11-27 16:31:55.775165Z	10.11.27.101	49174	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
791	2018-11-27 16:32:16.951624Z	10.11.27.101	49175	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
819	2018-11-27 16:35:15.773161Z	10.11.27.101	49176	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
834	2018-11-27 16:35:16.956086Z	10.11.27.101	49177	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
851	2018-11-27 16:35:28.180632Z	10.11.27.101	49178	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
881	2018-11-27 16:38:36.970744Z	10.11.27.101	49179	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
896	2018-11-27 16:38:38.192612Z	10.11.27.101	49180	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1191	2018-11-27 16:38:59.955126Z	10.11.27.101	49182	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1206	2018-11-27 16:38:57.918291Z	10.11.27.101	49186	185.244.156.230	443	TLSv1.2	187	Client Hello
1238	2018-11-27 16:39:18.344797Z	10.11.27.101	49187	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1257	2018-11-27 16:39:39.614811Z	10.11.27.101	49188	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1276	2018-11-27 16:39:41.332966Z	10.11.27.101	49189	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1295	2018-11-27 16:39:42.599833Z	10.11.27.101	49190	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1314	2018-11-27 16:39:43.833288Z	10.11.27.101	49191	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1339	2018-11-27 16:41:51.661210Z	10.11.27.101	49192	172.196.33.46	443	TLSv1.2	187	Client Hello
1366	2018-11-27 16:41:58.201320Z	10.11.27.101	49193	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1381	2018-11-27 16:41:59.312077Z	10.11.27.101	49194	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1400	2018-11-27 16:42:11.580287Z	10.11.27.101	49195	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1423	2018-11-27 16:44:11.387389Z	10.11.27.101	49196	185.158.251.55	443	TLSv1.2	187	Client Hello
1453	2018-11-27 16:45:19.388826Z	10.11.27.101	49197	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1468	2018-11-27 16:45:20.518186Z	10.11.27.101	49198	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1490	2018-11-27 16:46:43.699370Z	10.11.27.101	49199	174.34.253.11	443	TLSv1	187	Client Hello
1521	2018-11-27 16:48:40.535122Z	10.11.27.101	49200	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1536	2018-11-27 16:48:41.782532Z	10.11.27.101	49201	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1558	2018-11-27 16:50:54.352748Z	10.11.27.101	49202	185.244.156.230	443	TLSv1.2	219	Client Hello
1589	2018-11-27 16:52:01.778019Z	10.11.27.101	49203	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1684	2018-11-27 16:52:02.987445Z	10.11.27.101	49204	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1627	2018-11-27 16:53:42.254443Z	10.11.27.101	49205	172.196.33.46	443	TLSv1.2	219	Client Hello
1658	2018-11-27 16:55:23.806214Z	10.11.27.101	49206	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1673	2018-11-27 16:55:24.284732Z	10.11.27.101	49207	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1688	2018-11-27 16:55:47.888914Z	10.11.27.101	49208	185.158.251.55	443	TLSv1.2	219	Client Hello
1725	2018-11-27 16:58:37.890640Z	10.11.27.101	49209	174.34.253.11	443	TLSv1	181	Client Hello
1751	2018-11-27 16:58:44.260180Z	10.11.27.101	49210	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1766	2018-11-27 16:58:45.367784Z	10.11.27.101	49211	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1793	2018-11-27 17:02:05.397580Z	10.11.27.101	49212	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1808	2018-11-27 17:02:09.322585Z	10.11.27.101	49213	83.166.247.211	443	TLSv1.2	242	Client Hello (SNI=mautergase.com)
1831	2018-11-27 17:03:23.579528Z	10.11.27.101	49214	185.244.156.230	443	TLSv1.2	219	Client Hello

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.

The screenshot shows the ZeuS interface with a query session open. The query is `from 'traffic-with-dridex-infection.pcap' 1 event_type=="alert"`. The results are displayed in a table with 12 rows. The first row is highlighted in yellow. The table columns are: event_type, ts, src_ip, src_port, dest_ip, dest_port, and vlan. The first row shows an alert at 2018-11-27T17:03:23.729544Z from 185.244.150.238 to 10.11.27.101 on port 443.

event_type	ts	src_ip	src_port	dest_ip	dest_port	vlan
Alert (1)	2018-11-27T17:03:23.729544Z	185.244.150.238	443	10.11.27.101	49214	
Alert (1)	2018-11-27T16:50:54.499835Z	185.244.150.238	443	10.11.27.101	49202	
Alert (1)	2018-11-27T16:38:58.060802Z	185.244.150.238	443	10.11.27.101	49186	
Alert (2)	2018-11-27T16:38:39.580554Z	10.11.27.101	49181	95.181.198.231	80	
Alert (2)	2018-11-27T16:31:40.696707Z	10.11.27.101	53426	208.67.222.222	53	
Alert (2)	2018-11-27T16:31:40.666439Z	10.11.27.101	53425	208.67.222.222	53	
Alert (1)	2018-11-27T16:30:40.146287Z	10.11.27.101	49161	176.32.33.108	80	
Alert (1)	2018-11-27T16:30:37.597489Z	10.11.27.101	49159	176.32.33.108	80	
Alert (1)	2018-11-27T16:30:37.597489Z	10.11.27.101	49159	176.32.33.108	80	
Alert (1)	2018-11-27T16:30:15.757665Z	95.181.198.231	80	10.11.27.101	49158	
Alert (1)	2018-11-27T16:30:15.757665Z	95.181.198.231	80	10.11.27.101	49158	
Alert (3)	2018-11-27T16:30:15.757665Z	95.181.198.231	80	10.11.27.101	49158	

```
event_type: Alert (1),
ts: 2018-11-27T17:03:23.729544Z,
src_ip: 185.244.150.238,
src_port: 443 (port(uint16)),
dest_ip: 10.11.27.101,
dest_port: 49214 (port(uint16)),
vlan: null (uint16),
proto: "TCP",
app_proto: "tls",
alert: {
  severity: 1 (uint16),
  signature: "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)",
  category: "Domain Observed Used for C2 Detected",
  action: "allowed",
  signature_id: 2022627 (uint64),
  gid: 1 (uint64),
  rev: 12 (uint64),
  metadata: {
    signature_severity: ["Major"],
    former_category: null (string),
    attack_target: ["Client_and_Server"],
    deployment: ["Perimeter"],
    affected_product: null (string),
    created_at: ["2016_03_17"],
    performance: null (string)
  }
}
```

```
event_type: Alert (1),
ts: 2018-11-27T16:30:40.146287Z,
src_ip: 10.11.27.101,
src_port: 49161 (port(uint16)),
dest_ip: 176.32.33.108,
dest_port: 80 (port(uint16)),
vlan: null (uint16),
proto: "TCP",
app_proto: "http",
alert: {
  severity: 1 (uint16),
  signature: "ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)",
  category: "Malware Command and control Activity Detected",
  action: "allowed",
  signature_id: 2033203 (uint64),
  gid: 1 (uint64),
  rev: 7 (uint64),
  metadata: {
    signature_severity: ["Major"],
    former_category: null (string),
    attack_target: ["Client_Endpoint"],
    deployment: ["Perimeter"],
    affected_product: ["Windows_XP_Vista_7_8_10_Server_32_64_Bit"],
    created_at: null (string)
  }
}
```



```

event_type: alert (1),
ts: 2018-11-27T16:30:15.757665Z,
src_ip: 95.181.198.231,
src_port: 80 (port=(uint16)),
dest_ip: 10.11.27.101,
dest_port: 49158 (ports=(uint16)),
vlan: null ((uint16)),
proto: "TCP",
app_proto: "http",
alert: v {
  severity: 1 (uint16),
  signature: "ET MALWARE Likely Evil EXE download from MSXMLHTTP non-exe extension M2",
  category: "A Network Trojan was detected",
  action: "allowed",
  signature_id: 2022053 (uint64),
  gid: 1 (uint64),
  rev: 2 (uint64),
  metadata: > {signature_severity: ["Major"], former_category: null ((string)), attack_target: null ((string)), deployment: null ((string)), affected_product: null ((string)), created_at: ["2015_11_09"], performance_imp
},

```

```

event_type: alert (1),
ts: 2018-11-27T16:30:15.757665Z,
src_ip: 95.181.198.231,
src_port: 80 (port=(uint16)),
dest_ip: 10.11.27.101,
dest_port: 49158 (ports=(uint16)),
vlan: null ((uint16)),
proto: "TCP",
app_proto: "http",
alert: v {
  severity: 1 (uint16),
  signature: "ET POLICY PE EXE or DLL Windows file download HTTP",
  category: "Potential Corporate Privacy Violation",
  action: "allowed",
  signature_id: 2018959 (uint64),
  gid: 1 (uint64),
  rev: 5 (uint64),
  metadata: > {signature_severity: ["Informational"], former_category: null ((string)), attack_target: null ((string)), deployment: null ((string)), affected_product: null ((string)), created_at: ["2014_08_19"], perform
},

```

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 cochrinato.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.