Threat Analysis: Active C2 Discovery Using Protocol Emulation Part4 (Dacls, aka MATA)

By Takahiro Haruyama

Published: 2022-11-21 · Archived: 2026-04-05 21:03:59 UTC

Dacls, aka MATA, is a cross-platform RAT used by the DPRK-linked Lazarus Group and the first artifacts were observed around April 2018. The VMware Threat Analysis Unit (TAU) first discovered the Dacls C2 servers on the Internet by protocol emulation in August 2020. TAU is providing details here on how to detect the C2 servers and the scanning result.

Dacls C2 Protocol Initial Communication

In late 2019, 360 Netlab published the technical details of Dacls, including its C2 protocol details. The C2 protocol utilizes TLS and RC4 double-layer encryption. After establishing a TLS connection, Dacls beacons to the C2 server and then exchanges a key for the RC4 encryption. The initial communication between the Dacls client and C2 is shown in Figure 1.

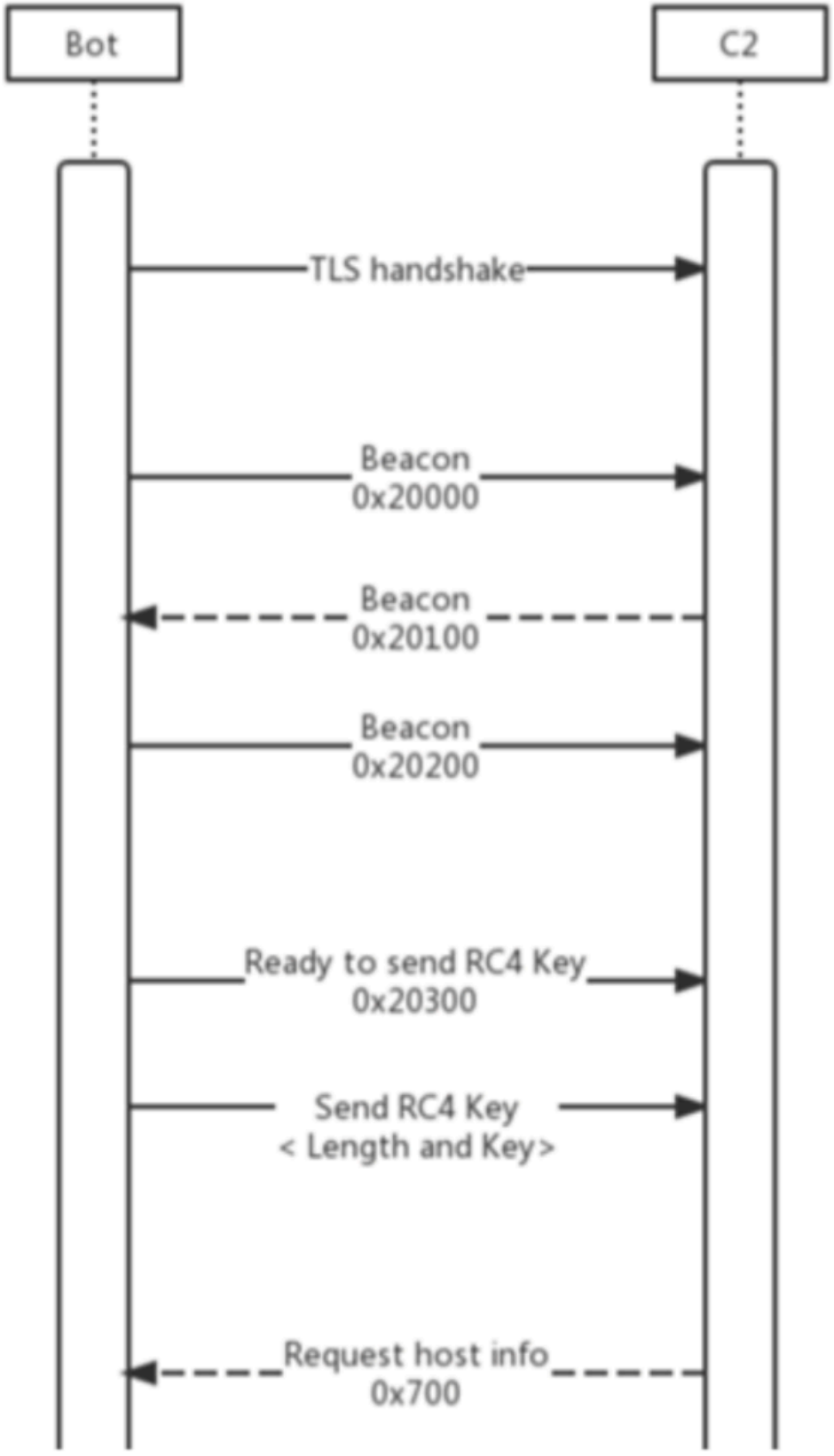

Figure 1: Dacls initial communication phase (source: 360 Netlab blog)

The beacon packet size is 4 bytes and the data referred to as an “opcode” is sent in little endian. After beaconing (0x20000/0x20100/0x20200), the Dacls client sends 12 bytes of data whose first 4 bytes data is an opcode (0x20300) telling the C2 to send an RC4 key and the remaining data is just null bytes. Following that, a randomly-generated RC4 key is sent with its size information as the size is also random.

After the RC4 key is exchanged, the communication is encrypted with RC4. The Dacls client waits for a command (opcode) from the C2. The first command can be 0x602 (config download), 0x900 (heartbeat), or 0x700 (sending host information), based on code analysis, but TAU has observed that the C2 always sends 0x700 first.

```
switch ( c2cmd[0] )
{
  case 0x602:
    if ( c2cmd[1] != 0x8E14 )
      goto LABEL_24;
    if ( !(unsigned int)MataRecv(__src, 0x8E14, 0xB4u) )
      goto LABEL_64;
    CopyConfigAndConvertEndian(__src, v22);
    payload[0] = SaveConfig(v22);
    if ( payload[0] )
    {
      MataSendPacket(0x20600, payload, 4LL);
      goto LABEL_64;
    }
    break;
  case 0x900:
    break;
  case 0x700:
    BaseInfo = GetBaseInfo((__int64)__src);
    LODWORD(__src[0]) = v2;
    if ( BaseInfo )
    {
      len = 0x550LL;
      status_code = 0x20500;
      baseinfo = __src;
    }
    else
    {
      status_code = 0x20600;
      baseinfo = 0LL;
      len = 0LL;
    }
    if ( (unsigned int)MataSendPacket(status_code, baseinfo, len) )
      v2 = 0;
    goto LABEL_64;
  default:
    goto LABEL_24;
}
```

Figure 2: Dacls C2 command loop

Last but not least, Dacls RAT implements a server mode. However, all IPs discovered by TAU's C2 scanner likely belong to hosted service providers, so we don't have to consider the possibility of server mode infections. Kaspersky also pointed out that the server mode was never used.

Threat Actor in Operation?

TAU implemented a scanner emulating the Dacls initial communication and then scanned the Internet to discover active Dacls C2 servers.

It should be noted that the C2 doesn't always send the command after the RC4 key exchange. Some servers send 0x700 and others do not. Besides, one server sometimes sends and sometimes doesn't. For instance, 35.246.189[.]81 always sends 0x700 but 23.94.139[.]92 and 172.87.222[.]3 only send it in the specific time as shown in the following logs. TAU hypothesizes that the first command is sent only when the threat actor is in operation.

———

[35.246.189.81]
2021/04/15 15:13:14,35.246.189.81,active,00010200
2021/04/15 15:13:15,35.246.189.81,active,RC4 key exchanged,00070000000000000000000000
2021/05/06 01:55:32,35.246.189.81,active,00010200
2021/05/06 01:55:32,35.246.189.81,active,RC4 key exchanged,00070000000000000000000000
2021/05/10 22:02:37,35.246.189.81,active,00010200
2021/05/10 22:02:38,35.246.189.81,active,RC4 key exchanged,00070000000000000000000000
2021/05/28 00:24:58,35.246.189.81,active,00010200
2021/05/28 00:24:59,35.246.189.81,active,RC4 key exchanged,00070000000000000000000000
2021/06/06 05:52:04,35.246.189.81,active,00010200
2021/06/06 05:52:04,35.246.189.81,active,RC4 key exchanged,00070000000000000000000000
2021/06/24 09:08:13,35.246.189.81,active,00010200
2021/06/24 09:08:14,35.246.189.81,active,RC4 key exchanged,00070000000000000000000000
2021/07/06 23:01:24,35.246.189.81,active,00010200
2021/07/06 23:01:25,35.246.189.81,active,RC4 key exchanged,00070000000000000000000000
2021/08/03 22:01:09,35.246.189.81,active,00010200
2021/08/03 22:01:10,35.246.189.81,active,RC4 key exchanged,00070000000000000000000000
2021/08/30 03:55:55,35.246.189.81,active,00010200
2021/08/30 03:55:56,35.246.189.81,active,RC4 key exchanged,00070000000000000000000000

[23.94.139.92]
2021/01/17 14:25:15,23.94.139.92,active,00010200
2021/02/11 00:46:27,23.94.139.92,active,00010200
2021/02/11 00:46:33,23.94.139.92,active,RC4 key exchanged,00070000000000001fdc28ef
2021/02/21 18:50:53,23.94.139.92,active,00010200

[172.87.222.3]
2020/11/25 18:09:53,172.87.222.3,active,00010200
2020/11/25 18:10:07,172.87.222.3,active,RC4 key exchanged,00070000000000005e10795b
2020/12/09 07:03:26,172.87.222.3,active,00010200
2020/12/09 07:03:36,172.87.222.3,active,RC4 key exchanged,000700000000000068f4492b
2020/12/26 19:37:18,172.87.222.3,active,00010200
2021/01/05 06:15:09,172.87.222.3,active,00010200
2021/01/05 06:15:21,172.87.222.3,active,RC4 key exchanged,0007000000000000b9dc64f4
2021/01/17 02:59:35,172.87.222.3,active,00010200
2021/02/11 18:53:29,172.87.222.3,active,00010200
2021/02/23 20:45:35,172.87.222.3,active,00010200

———

Our C2 scanner detects IPs sending back the RC4-encrypted command (0x700), and those just returning the beacon (0x20100) as the Dacls C2 servers. The detection condition may cause false positives but there has been no issue since the discovered C2 IOCs started to be utilized by our endpoint products in September 2020.

Wrap-up

By emulating the Dacls C2 protocol and scanning the Internet, TAU has identified 121 Dacls C2 servers over the past 2 years. The discovered C2 IOCs are available on our GitHub page. The Dacls active C2s have been declining, but multiple C2s are still active now. TAU will continue tracking the malware infrastructure in real-time as long as the threat actor uses it.
