White Paper

How Corelight helps analysts find command and control activity

Introduction

When malware establishes an initial foothold in a target organization one of its next steps is to establish communication with a command and control (C2) server for further instruction. This communication continues, often at regularly scheduled intervals, so that adversaries can stage additional payloads, move laterally, and ultimately exfiltrate data.

The network, given its breadth and depth of communication visibility, offers a strong vantage point from which defenders can spot C2 activity. Advanced adversaries, however, use a variety of techniques to obfuscate C2 traffic, such as encryption, tunneling in noisy protocols like DNS, or using domain generation algorithms to evade blacklists.

Identifying C2 activity requires both comprehensive network security monitoring and durable detections that can track adversaries regardless of port, protocol or domain. Corelight delivers these capabilities in spades, turning packets into protocol-comprehensive evidence and generating over 50 unique detections and insights covering both known C2 toolkits and novel C2 infrastructure.

With the Corelight C2 Collection analysts get the visibility and the detections they need to reliably identify command and control activity in their environment.

Finding C2s with Corelight evidence

Corelight transforms traffic into dozens of rich protocol logs that summarize activity on the wire so analysts can easily follow a given connection across ports and protocols. Corelight provides this evidence even where traffic is encrypted, by parsing the observable characteristics of the connection and certificate details. Threat hunters using Corelight have access to evidence for both unencrypted and encrypted protocols favored for C2 communication channels, including:

- HTTP
- DNS
- ICMP
- SSL
- SSH
- And more..

Each of Corelight's protocol logs are packed with security-useful data fields that cover visibility gaps left by common network appliance logs. The additional protocol evidence Corelight provides can be crucial for hunters looking to identify C2 activity in the wild. Consider the difference in information depth between a Corelight dns.log and a typical log generated by a DNS server in the diagrams below:

Diagram 1: A sample Corelight dns.log

```
1308930716.700706 CNFhPo1bq5dJD3wzJ6
172.16.238.131 54304 172.16.238.2 53 udp 27628
0.004850 maps.google.com 1 C_INTERNET 1 A
0 NOERROR F F T T 0 maps.l.google.
Com,74.125.225.81,74.125.225.82,74.125.225.83,74
.125.225.84,74.125.225.80
5.000000,5.000000,5.000000,5.000000,5.00
0000,5.000000 F
```

Diagram 2: A sample DNS server log

```
client 192.168.117.234#53311: view authoritative:
query: example.org IN NS -EDC 192.168.36.217)
```

Notably, the Corelight dns.log contains the full content of response to the DNS query, a detail often missing from DNS server records. By capturing both the full DNS query and response, Corelight gives threat hunters the evidence needed to find C2s communications tunneling over DNS. For example, an analyst using a SIEM can easily query their Corelight DNS.logs, filter to identify chatty hosts and then inspect the DNS responses returned, which reveal nonstandard, alphanumeric DNS response strings indicative of C2 server instructions.

Finding C2s with Corelight detections and insights

The Corelight C2 Collection helps analysts locate command and control activity with over 50 unique insights and detections. Battle-tested by some of the world's most sophisticated organizations, this collection covers both known C2 toolkits and MITRE ATT&CK C2 techniques to find novel attacks. Corelight covers:

HTTP C2	Detect known families of malware that conduct C2 communications over HTTP, such as Powershell Empire and Cobalt Strike
DNS Tunneling	Detect DNS tunneling behavior and specific tunneling tools such as iodine

ICMP Tunneling	Detect ICMP tunneling behavior as well as the presence of specific tunneling tools such as ICMP Shell
Domain Generation Algorithms	Detect C2 traffic based on DNS activity from malware using Domain Generation Algorithms
Meterpreter	Detect C2 activity from Metasploit's Meterpreter shell across HTTP and generic TCP/UDP traffic

For example, Corelight's HTTP C2 detection capabilities can reveal more than a dozen malware toolkits. A skeptic might say: "yes, but don't attackers use HTTPS?" Some will of course encrypt their C2, but note that this encryption also introduces more work to implement and creates additional evidence around the encryption that defenders can use to track and identify them, such as JA3 fingerprints.

In many cases it's easier and can be more effective to impersonate a browser or appliance using HTTP and hide C2 communications amidst the HTTP noise. Corelight's approach to detecting the C2 goes beyond signatures to more durable behavioral analyses that target artifacts like the structure of the HTTP headers. Corelight's detections generate new notice.log entries and analysts can pivot via the connection UID in these notices to Corelight's http.log and beyond for further investigation.

Diagram 3: A sample Corelight notice.log alert for Trickbot malware HTTP C2 traffic:

```
{ [-]
   _path: notice
   [...]
   msg: Potential C2 traffic - Trickbot Malware. the POST content includes 'os password' .  https://attack.mitre.org
        /software/S0266/. This detection is based on attributes within the http connection, further details can be
        found in http.log and conn.log - the relevant log lines will share the same uid as this notice.  (Algorithm 2)
   note: HTTP_C2::C2_Traffic_Observed
   [...]
   severity.level: 1
   severity.name: alert
   [...]
}
```

In Diagram 3 you see a Corelight C2 notice.log generated for Trickbot malware that's also providing the credentials ('os password') for the compromised machine. By next pivoting into the Corelight's http.log connected to the alert the analyst can also see the password string contained in the post body:

Diagram 4: Corelight http.log for the connection related to the HTTP c2 notice

```
{ [-]
   _path: http
   [...]
   post_body: SKINNER-WIN-PC\willy.skinner|P@ssw0rd$\x00os passwords
   [...]
}
```

In this example, Corelight has generated both the alert (HTTP C2 detection) as well as the evidence needed to validate the alert in a single, integrated data source, accessible from just a couple of clicks!

For more detailed information about the Corelight C2 Collection, please contact us.