Breaking the Ice: Detecting IcedID and Cobalt Strike Beacon with Network Detection and Response (NDR)

awakesecurity.com/blog/detecting-icedid-and-cobalt-strike-beacon-with-network-detection-and-response/

April 8, 2021

Blog Post

It has become something of an Internet meme that Cobalt Strike is everywhere. Cobalt Strike Beacon is seen in a myriad of investigations, so security operations as well as incident response teams must be able to detect and effectively remediate this heavily utilized post exploitation tool. Arista's Awake Labs team encounters IcedID and Cobalt Strike Beacon both in our incident response and managed network detection and response (MNDR) engagements. In this blog, we provide details of a detection and investigation of Cobalt Strike Beacon using the Awake network detection and response platform, which ultimately uncovered an IcedID infection.

Initial Alert

An adversarial model in the Awake Security Platform alerted the Managed Network Detection and Response (MNDR) team to ***C2: TLS Characteristic of Cobalt Strike to Domain***. The same activity also triggered a model that the MNDR team uses to trigger threat hunts – ***C2: Multiple Activities to Newly Seen Domain Created Within Last Year***.

Connection Analysis

The offending TLS connection was to the domain: *mazaksaedr23[.]space*. Looking at the connection details, we identified that the self-signed certificate being used by the server had default values for the certificate attributes (Figure 1). This, along with the recency of the certificate validation date raised our suspicions. Looking up the client JA3 hash indicated the connection may have been initiated from Microsoft Excel.

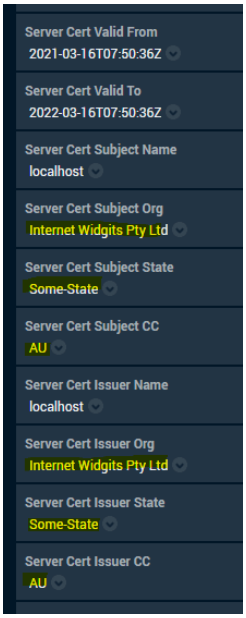

Figure 1: TLS Characteristics of Initial Connection

When analyzing the domain within the Awake platform, we saw that it was first observed within this customer environment very recently, registered recently, and registered with Porkbun using Private by Design, LLC (Figure 2).

Figure 2: Domain Registration Details for C2 domain

We also identified ongoing connections to this domain every 5 minutes, a steady and clear beaconing pattern from the source device.

Timeline Analysis

The next step was to perform timeline analysis and investigate what caused the initial connection. From the initial connection, we were able to quickly pivot by leveraging the pre-built +/- 1-minute search window within the Awake platform (Figure 3).

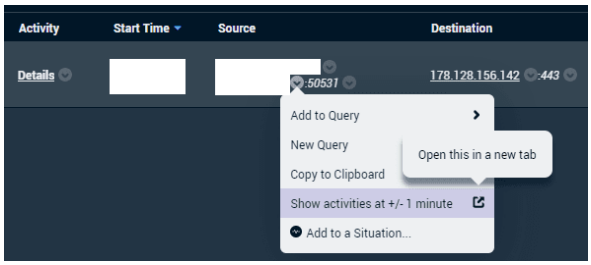

Figure 3: Pivoting to Construct the Attack Timeline

We identified a prior connection towards *lapoedjkeo[.]top* – which had the same certificate information and IP address. We did not see beaconing to this domain during our investigation. However, a connection to *217rotebenl[.]online*, another highly suspicious domain, closely preceded the connection to the "*.top"* domain. Figure 4 is a screenshot of the PCAP data for that connection, as shown in the Awake platform. The PCAP was also exported from the platform for evidence preservation.

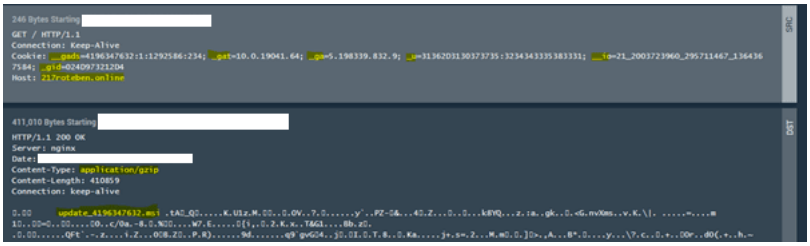

Figure 4: PCAP of Traffic to Suspect Domain

The key pieces of information that raised our suspicions of IcedID are highlighted in Figure 4. Firstly, based on threat intelligence we recognized the cookie names and order: **__gads**, **_gat**, **_ga**, **_u**, **__io** and **_gid** to be reminiscent of IcedID. In addition, it was notable that the content type shown was 'application/gzip'. While looking at the PCAP data in hex within the Awake platform shows the expected GZIP file header of 0x1f 0x8b (Figure 5), extracting and expanding the contents through normal means failed.

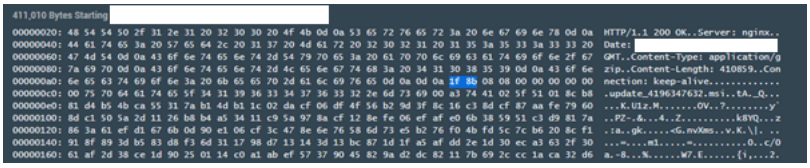

Figure 5: PCAP Analysis shows GZIP File Header

We recognized this activity to be like that documented in the excellent write up from BinaryDefense, also linking IcedID and Cobalt Strike. Using the tool 'IcedDecrypt' we were able to pull out the IcedID configuration information (Figure 6); useful for investigation and hunting on the endpoint side.

Figure 6: IcedID Configuration Information

Expanding the Scope

Next, we looked at when the first connection to *217roteben[.]online* was made and pivoted around this connection to identify the cause. We saw HTTP GET requests to three different IP addresses that downloaded interestingly named DAT files (Figure 7).

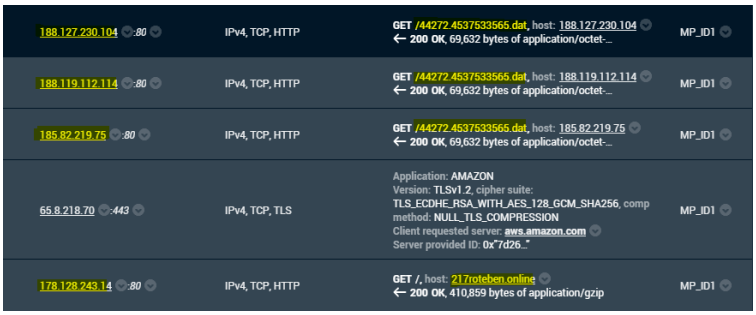

Figure 7: Downloads of IcedID Masquerading as DAT Files

Again, by looking at the PCAP data, we can see these files were executables. We exported the PCAP and determined this file was IcedID (Figure 8).

Figure 8: PCAP Showing the IcedID Executable

We were able to identify one other device that was compromised later that same day, by identifying the same traffic patterns.

After just under 24 hours, the beaconing to *mazaksaedr23[.]space* stopped. Shortly after this, there was another alert for ***C2: TLS Characteristic of Cobalt Strike to Domain***, this time for a different domain: *agitopinaholop[.]uno*, which immediately continued the C2 beaconing pattern. This domain had the same TLS certificate information as *mazaksaedr23[.]space*, with slightly earlier validity dates.

Summary and Conclusion

Even without decryption, Cobalt Strike Beacon can be detected on the network side, precisely *because* TLS was used. Within a very short amount of time, we were able to map out the attack from the network side and provide the customer with network and endpoint IOCs to aid their investigation and remediation efforts.

Threat Hunting for IcedID and Cobalt Strike

Based on this activity, the MNDR team used additional threat hunting models to search across our other customers. Here is what we based these models on:

Detecting	Threat hunting triggers
IcedID	HTTP requests with the cookie names: __gads, _gat, _ga, _u, __io, _gidin that exact order.
IcedID	The .DAT file in the request URI. Here, we can use a regular expression, such as: /^\/[0-9]{5}\.[0-9]{10}\.dat$/This will identify a request URI with 5 digits, followed by a '.', followed by 10 digits, with a '.dat' extension
Cobalt Strike Beacon in this instance; could be used by other malware	TLS connections with anomalies in the server certificate e.g. TLS connections to servers with default certificate information being used
The connection order seen in this infection chain	Activity towards domains with uncommon TLDs within a short period of time. In this instance: a domain ending in ".online", a domain ending in ".space", a domain ending in ".top".All from the same source device, where the connections occurred within a 2-minute window.

Network IOCs

The following can be used as network IOCs for the described activity:

IOC	Type	Detecting
mazaksaedr23[.]space	Domain	Cobalt Strike Beacon
agitopinaholop[.]uno	Domain	Cobalt Strike Beacon
lapoedjkeo[.]top	Domain	Cobalt Strike Beacon
178.128.156[.]142	IPv4 address	IPv4 address associated with mazaksaedr23[.]space and lapoedjkeo[.]top
165.227.28[.]47	IPv4 address	IPv4 address associated with agitopinaholop[.]uno
217roteben[.]online	Domain	IcedID
178.128.243[.]14	IPv4 address	IPv4 address associated with 217roteben[.]online
188.127.230[.]104	IPv4 address	IcedID
188.119.112[.]114	IPv4 address	IcedID
185.82.219[.]75	IPv4 address	IcedID
188.119.112[.]125	IPv4 address	IcedID
185.82.219[.]80	IPv4 address	IcedID
188.127.230[.]133	IPv4 address	IcedID
[.]savps[.]ru	Email address	IcedID – Email address from SSL Certificate attached to the POP3/110 and IMAP/993 services on 188.127.230.133

Host based IOCs

The following can be used as IOCs to hunt for this specific activity on the host, although the configuration is likely changeable.

IOC	Type	Detecting
QuarterArctic	Directory	IcedID
blast_x32.dat	DLL file	IcedID

license.dat	Associated file	IcedID
rundll32.exe “%localappdata%/blast_x32.dat”,update /i “QuarterArctic/license.dat”	Command line	IcedID
Rundll32Execution.txt	Associated file	IcedID

Subscribe!

If you liked what you just read, subscribe to hear about our threat research and security analysis.

Kieran Evans

Threat Hunting and Incident Response Specialist

LinkedIn