Security Incident Report

Low

HI_CLIENT_IIS_DELIMITER

Customer	ntts-cis-dev (こんにちは)	
Device	NEBULA-POC-01	
Signature	HI_CLIENT_IIS_DELIMITER	
Severity	**Confidence**	**Reference #**
Low	Max	16075643665517812

Date and Time			
Start Date	2017-09-05 07:17:41.000 UTC	**End Date**	2017-09-05 07:17:41.000 UTC

Description

The host 1.1.1.1 has triggered the signature "HI_CLIENT_IIS_DELIMITER" which is often seen during server exploitation attempts. Since the attack has not been blocked, we recommend that an impact analysis is performed. If possible we also recommend to block future triggers of this specific signature.

An extract of the NIDS activity noted by the source is listed in the table below:

Date/Time	Source IP	Destination IP	Signature	Action
2017-09-05 07:17:41 UTC	1.1.1.1	192.168.218.99	HI_CLIENT_IIS_DELIMITER	ACCEPT

Recommendation/Action

Based on the activity noted in this report, NTT Security recommends the following actions:

Block access from potentially malicious hosts*
Block access from 10[.]43[.]2[.]149 to prevent further interaction with this potentially malicious host. Please note that we recommend an impact analysis before blocking communication since this may disrupt services which are critical to your organization.The block action needs to be taken on all applicable gateway appliances (Firewall, Proxy or similar system) in order to be effective.

Apply block action for attack signature
Investigate if it is possible to apply a block action for the attack signature "HI_CLIENT_IIS_DELIMITER" without putting your environment at risk. A common method is to evaluate the historical false positive rate, impact of a false positive, and possibly exclude resources which have high uptime requirements.

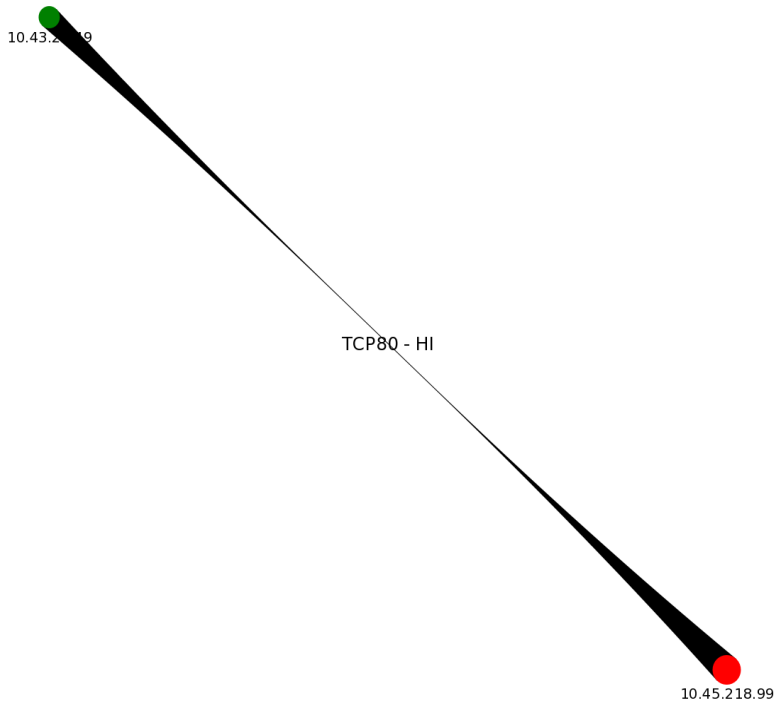
Log file investigation
Investigate and attempt to identify any additional connections to and from the server 192.168.218.99 from the time of the above activity. Typically this would include searching through logs from sources such as Proxy, Firewall and DNS. Please make sure that the logs are correctly timestamped (timezone/NTP) so that the relevant logs are covered by the searches.

*Active Response API action available. It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here', making it look like readable English. Many desktop publishing packages and web page editors now use Lorem Ipsum as their default model text, and a search for 'lorem ipsum' will uncover many web sites still in their infancy. Various versions have evolved over the years, sometimes by accident, sometimes on purpose, is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of

Low

Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum

Access Patterns



Details	
Signature(s)	HI_CLIENT_IIS_DELIMITER
Log source(s)	cisco:firepower:sensor:syslog
Src Hosts	N/A
Src IPv4 addresses	1.1.1.1
Dest Hosts	N/A
Dest IPv4 addresses	192.168.218.99
Asset Details	N/A
ARA Recommendation	coa Type: PERIMETER_BLOCKING coa Observable Address_Value: 1.1.1.1