

# \_General

Created by Dennis Underwood, last modified by Kyle Nehman on Jun 12, 2025

| Domain                              | Port | Protocol | Component       | Producers of Traffic                                                                                                                                       | Purpose                                                                                                                                                                                                                                  | Certificate Validation/Revocation Domains (as of 1 May 2024)                                                                                    |
|-------------------------------------|------|----------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| dashboard.cybercrucible.com         | 443  | HTTPS    | Web Application | Users, typically assigned members of the IT, Security, and Compliance teams, who manage Cyber Crucible software. This web application is built on ReactJS. | This domain is tied to the administration panel for Cyber Crucible software. This admin panel is used to manage all licenses, and software agents. It is used to investigate and observe potential data or identity extortion incidents. | OCSP URL: <a href="http://r3.o.lencr.org">http://r3.o.lencr.org</a><br>CA URL/Issuer: <a href="http://r3.i.lencr.org">http://r3.i.lencr.org</a> |
| agent.tasking.rpp.cybercrucible.com | 443  | HTTPS    | Windows Service | Cyber Crucible software agents use this domain. Users do not interact with this server, and this server is managed by a separate Federated ID allocation.  | Cyber Crucible software agents use this domain to receive tasking, and submit data to the agent-specific REST server.                                                                                                                    | OCSP URL: <a href="http://r3.o.lencr.org">http://r3.o.lencr.org</a><br>CA URL/Issuer: <a href="http://r3.i.lencr.org">http://r3.i.lencr.org</a> |

|                                     |     |       |                 |                                                                                                                                  |                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-----|-------|-----------------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cognito-idp.us-west-2.amazonaws.com | 443 | HTTPS | Web Application | Users of the web application, or custom REST API calls by a client will produce traffic to the AWS Cognito service during login. | Cyber Crucible currently uses AWS Cognito for user pool and Federated Identity services, in support of software, REST API, and user OAuth 2.0 protected communications and user management. | <p>CRL distribution URL:<br/> <a href="http://crl.r2m03.amazontrust.com/r2m03.crl">http://crl.r2m03.amazontrust.com/r2m03.crl</a></p> <p>OCSP URL:<br/> <a href="http://ocsp.r2m03.amazontrust.com">http://ocsp.r2m03.amazontrust.com</a></p> <p>CA URL/Issuer:<br/> <a href="http://crt.r2m03.amazontrust.com/r2m03.cer">http://crt.r2m03.amazontrust.com/r2m03.cer</a></p> <p>CRL distribution URL:<br/> <a href="http://crl.r2m02.amazontrust.com/r2m02.crl">http://crl.r2m02.amazontrust.com/r2m02.crl</a></p> <p>OCSP URL/Issuer:<br/> <a href="http://ocsp.r2m02.amazontrust.com">http://ocsp.r2m02.amazontrust.com</a></p> <p>CRL distribution URL:<br/> <a href="http://crt.r2m02.amazontrust.com/r2m02.cer">http://crt.r2m02.amazontrust.com/r2m02.cer</a></p> |
|-------------------------------------|-----|-------|-----------------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                 |     |       |                    |                                                                                                                                                                |                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------|-----|-------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ransomware<br>wind.auth.us-<br>west-<br>2.amazoncogn<br>ito.com | 443 | HTTPS | Web<br>Application | Users of the<br>web<br>application, or<br>custom REST<br>API calls by a<br>client will<br>produce traffic<br>to the AWS<br>Cognito<br>service during<br>login. | Cyber Crucible<br>currently uses<br>AWS Cognito<br>for user pool<br>and Federated<br>Identity<br>services, in<br>support of<br>software,<br>REST API, and<br>user oAuth 2.0<br>protected<br>communicatio<br>ns and user<br>management. | <p>CRL<br/>distribution<br/>URL:<br/><a href="http://crl.r2m03.amazontrust.com/r2m03.crl">http://crl.r2m03.amazontrust.com/r2m03.crl</a></p> <p>OCSP URL:<br/><a href="http://ocsp.r2m03.amazontrust.com">http://ocsp.r2m03.amazontrust.com</a></p> <p>CA URL/Issuer:<br/><a href="http://crt.r2m03.amazontrust.com/r2m03.cer">http://crt.r2m03.amazontrust.com/r2m03.cer</a></p> <p>CRL<br/>distribution<br/>URL:<br/><a href="http://crl.r2m02.amazontrust.com/r2m02.crl">http://crl.r2m02.amazontrust.com/r2m02.crl</a></p> <p>OCSP<br/>URL/Issuer:<br/><a href="http://ocsp.r2m02.amazontrust.com">http://ocsp.r2m02.amazontrust.com</a></p> <p>CRL<br/>distribution<br/>URL:<br/><a href="http://crt.r2m02.amazontrust.com/r2m02.cer">http://crt.r2m02.amazontrust.com/r2m02.cer</a></p> |
|-----------------------------------------------------------------|-----|-------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                              |     |       |                 |                                                                               |                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------|-----------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">ransomwarere</a><br><a href="#">wind-</a><br><a href="#">agents.auth.u</a><br><a href="#">s-west-</a><br><a href="#">2.amazoncogn</a><br><a href="#">ito.com</a><br>(deprecated) | 443 | HTTPS | Windows Service | Cyber Crucible software agents use this domain. Users do not use this domain. | Cyber Crucible software agents use this domain, which is AWS Cognito, for user pool and Federated Identity services, in support of their OAuth 2.0 protected communications and software management. | CRL distribution URL:<br><a href="http://crl.r2m03.amazontrust.com/r2m03.crl">http://crl.r2m03.amazontrust.com/r2m03.crl</a><br>OCSP URL:<br><a href="http://ocsp.r2m03.amazontrust.com">http://ocsp.r2m03.amazontrust.com</a><br>CA URL/Issuer:<br><a href="http://crt.r2m03.amazontrust.com/r2m03.cer">http://crt.r2m03.amazontrust.com/r2m03.cer</a><br>CRL distribution URL:<br><a href="http://crl.r2m02.amazontrust.com/r2m02.crl">http://crl.r2m02.amazontrust.com/r2m02.crl</a><br>OCSP URL/Issuer:<br><a href="http://ocsp.r2m02.amazontrust.com">http://ocsp.r2m02.amazontrust.com</a><br>CRL distribution URL:<br><a href="http://crt.r2m02.amazontrust.com/r2m02.cer">http://crt.r2m02.amazontrust.com/r2m02.cer</a> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------|-----------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                            |     |       |                   |                                                                               |                                                                                                                                                                                 |                                                                                                                                                 |
|------------------------------------------------------------|-----|-------|-------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| agent.oauth.rpp.cybercrucible.com                          | 443 | HTTP  | Windows Service   | Cyber Crucible software agents use this domain. Users do not use this domain. | Cyber Crucible software agents use this domain for OAuth 2.0 protected communications and software management. This domain replaces the deprecated AWS Cognito OAuth url above. |                                                                                                                                                 |
| installerfiles.rpp.cybercrucible.com                       | 443 | HTTPS | HTTPS File Server | Cyber Crucible installation and update files (drivers, services, etc.)        | Cyber Crucible's installation and update files are stored in this website. It is used to do initial agent installation as well as fetch files for any required updates.         | OCSP URL: <a href="http://r3.o.lencr.org">http://r3.o.lencr.org</a><br>CA URL/Issuer: <a href="http://r3.i.lencr.org">http://r3.i.lencr.org</a> |
| <a href="http://ipv4.icanhazip.com">ipv4.icanhazip.com</a> | 443 | HTTPS | Windows Service   | Cyber Crucible software agents use this domain.                               | Cyber Crucible software agents query this domain to correlate the IPv4 WAN address for an agent.                                                                                | OCSP URL: <a href="http://r3.o.lencr.org">http://r3.o.lencr.org</a><br>CA URL/Issuer: <a href="http://r3.i.lencr.org">http://r3.i.lencr.org</a> |
| ipv6.icanhazip.com                                         | 443 | HTTPS | Windows Service   | Cyber Crucible software agents use this domain.                               | Cyber Crucible software agents query this domain to correlate the IPv6 WAN address for an agent.                                                                                | OCSP URL: <a href="http://r3.o.lencr.org">http://r3.o.lencr.org</a><br>CA URL/Issuer: <a href="http://r3.i.lencr.org">http://r3.i.lencr.org</a> |

|                         |    |      |                 |                                                                                |                                                                                                                                                                                                                                                            |  |
|-------------------------|----|------|-----------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| r3.o.lencr.org          | 80 | OCSP | Windows Service | Web application users and Cyber Crucible software agents both use this domain. | This domain is the Let's Encrypt TLS certificate validation and revocation check (OCSP) check server. Without access to this server, agents and the web application communications may not work.                                                           |  |
| rs.i.lencr.org          | 80 | HTTP | Windows Service | Web application users and Cyber Crucible software agents both use this domain. | This domain is the Let's Encrypt TLS Certificate Authority (CA) server, that is used by validate TLS certificates. Without access to this server, agents and the web application communications may not work.                                              |  |
| crl.r2m03.amazonaws.com | 80 | HTTP | Windows Service | Web application users and Cyber Crucible software agents both use this domain. | This domain is the Amazon Web Services (AWS) certificate validation and revocation check (CRL) server. Without access to this server, agents and web application users cannot gain validated credentials, to then access secured Cyber Crucible resources. |  |

|                          |    |      |                 |                                                                                |                                                                                                                                                                                                                                                             |  |
|--------------------------|----|------|-----------------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| crl.r2m02.amazonaws.com  | 80 | HTTP | Windows Service | Web application users and Cyber Crucible software agents both use this domain. | This domain is the Amazon Web Services (AWS) certificate validation and revocation check (CRL) server. Without access to this server, agents and web application users cannot gain validated credentials, to then access secured Cyber Crucible resources.  |  |
| ocsp.r2m03.amazonaws.com | 80 | OCSP | Windows Service | Web application users and Cyber Crucible software agents both use this domain. | This domain is the Amazon Web Services (AWS) certificate validation and revocation check (OCSP) server. Without access to this server, agents and web application users cannot gain validated credentials, to then access secured Cyber Crucible resources. |  |

|                             |    |      |                 |                                                                                |                                                                                                                                                                                                                                                                                  |  |
|-----------------------------|----|------|-----------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| ocsp.r2.m02.amazontrust.com | 80 | OCSP | Windows Service | Web application users and Cyber Crucible software agents both use this domain. | This domain is the Amazon Web Services (AWS) certificate validation and revocation check (OCSP) server. Without access to this server, agents and web application users cannot gain validated credentials, to then access secured Cyber Crucible resources.                      |  |
| crt.r2m03.amazontrust.com   | 80 | HTTP | Windows Service | Web application users and Cyber Crucible software agents both use this domain. | This domain is the Amazon Web Services (AWS) TLS Certificate Authority (CA) server, that is used by validate TLS certificates. Without access to this server, agents and the web application cannot gain validated credentials, to then access secured Cyber Crucible resources. |  |

|                                                  |     |       |                 |                                                                                                                                                           |                                                                                                                                                                                                                                                                                  |                                                                                                                                                 |
|--------------------------------------------------|-----|-------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| crt.r2m02.amazontrust.com                        | 80  | HTTP  | Windows Service | Web application users and Cyber Crucible software agents both use this domain.                                                                            | This domain is the Amazon Web Services (AWS) TLS Certificate Authority (CA) server, that is used by validate TLS certificates. Without access to this server, agents and the web application cannot gain validated credentials, to then access secured Cyber Crucible resources. |                                                                                                                                                 |
| v2-agent.tasking.ransomwarewind.com (deprecated) | 443 | HTTPS | Windows Service | Cyber Crucible software agents use this domain. Users do not interact with this server, and this server is managed by a separate Federated ID allocation. | Cyber Crucible software agents use this domain to receive tasking, and submit data to the agent-specific REST server.                                                                                                                                                            | OCSP URL: <a href="http://r3.o.lencr.org">http://r3.o.lencr.org</a><br>CA URL/Issuer: <a href="http://r3.i.lencr.org">http://r3.i.lencr.org</a> |

|                                                                                 |     |       |                    |                                        |                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------|-----|-------|--------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ransomware-rewind-installation-files-64.s3.us-west-2.amazonaws.com (deprecated) | 443 | HTTPS | AWS S3 File Server | Cyber Crucible installer file location | Cyber Crucible's installer exe is located in an S3 bucket hosted at this domain. This domain is likely only accessed if using the script installer. | <p>CRL distribution URL:<br/> <a href="http://crl.r2m03.amazontrust.com/r2m03.crl">http://crl.r2m03.amazontrust.com/r2m03.crl</a></p> <p>OCSP URL:<br/> <a href="http://ocsp.r2m03.amazontrust.com">http://ocsp.r2m03.amazontrust.com</a></p> <p>CA URL/Issuer:<br/> <a href="http://crt.r2m03.amazontrust.com/r2m03.cer">http://crt.r2m03.amazontrust.com/r2m03.cer</a></p> <p>CRL distribution URL:<br/> <a href="http://crl.r2m02.amazontrust.com/r2m02.crl">http://crl.r2m02.amazontrust.com/r2m02.crl</a></p> <p>OCSP URL/Issuer:<br/> <a href="http://ocsp.r2m02.amazontrust.com">http://ocsp.r2m02.amazontrust.com</a></p> <p>CRL distribution URL:<br/> <a href="http://crt.r2m02.amazontrust.com/r2m02.cer">http://crt.r2m02.amazontrust.com/r2m02.cer</a></p> |
|---------------------------------------------------------------------------------|-----|-------|--------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                     |     |       |                    |                                        |                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------|-----|-------|--------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">installerfiles.ransomwarewinder.com</a><br>(deprecated) | 443 | HTTPS | AWS S3 File Server | Cyber Crucible download and installers | Cyber Crucible's installation and update files are stored in this S3 bucket. It is used to do initial agent installation as well as fetch files for any required updates. | CRL distribution URL:<br><a href="http://crl.r2m03.amazontrust.com/r2m03.crl">http://crl.r2m03.amazontrust.com/r2m03.crl</a><br>OCSP URL:<br><a href="http://ocsp.r2m03.amazontrust.com">http://ocsp.r2m03.amazontrust.com</a><br>CA URL/Issuer:<br><a href="http://crt.r2m03.amazontrust.com/r2m03.cer">http://crt.r2m03.amazontrust.com/r2m03.cer</a><br>CRL distribution URL:<br><a href="http://crl.r2m02.amazontrust.com/r2m02.crl">http://crl.r2m02.amazontrust.com/r2m02.crl</a><br>OCSP URL/Issuer:<br><a href="http://ocsp.r2m02.amazontrust.com">http://ocsp.r2m02.amazontrust.com</a><br>CRL distribution URL:<br><a href="http://crt.r2m02.amazontrust.com/r2m02.cer">http://crt.r2m02.amazontrust.com/r2m02.cer</a> |
|---------------------------------------------------------------------|-----|-------|--------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                     |     |       |                 |                                                                                                                                                                                             |                                                                                                                                                             |                                                                                                                                                 |
|---------------------------------------------------------------------|-----|-------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">v2-web.tasking.ransomwarerewind.com</a><br>(deprecated) | 443 | HTTPS | Web Application | Users, typically assigned members of the IT, Security, and Compliance teams, who manage Cyber Crucible software. Custom REST API programs developed by customers will also use this domain. | This domain is the REST server which the ReactJS dashboard uses to dynamically create, retrieve, update, and delete relevant data from the web application. | OCSP URL: <a href="http://r3.o.lencr.org">http://r3.o.lencr.org</a><br>CA URL/Issuer: <a href="http://r3.i.lencr.org">http://r3.i.lencr.org</a> |
|---------------------------------------------------------------------|-----|-------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|

Revision #1  
Created 2026-05-18 20:27:06 UTC by Dennis Underwood  
Updated 2026-05-18 20:27:06 UTC by Dennis Underwood