

Anatomy of an Attack: Gaining Remote Access Using Valid Credentials

eSentire's Malkara VPN analytics engine identifies suspicious login activity through the use of machine learning

Threat Type:

Suspicious Remote Access
MITRE ATT&CK® Techniques:
- T1133 – External Remote Services
- T1078 – Valid Accounts

When adversaries obtain valid credentials, they can leverage external-facing remote services to gain unauthorized access and/or persist within a network.

Functionality:

Adversaries who have access to valid accounts, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network, leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.¹

The Threat:

- Temporary or permanent loss of sensitive or proprietary information
- Disruption to regular operations
- Financial losses incurred to restore systems and files
- Potential harm to an organization's reputation

Background: What Is Suspicious Remote Access?

With the increasing proliferation of the remote workforce, most organizations provide the ability for remote access into their networks, either via VPN, Citrix, or other access mechanisms. External remote services allow users to connect to internal network resources from external locations. Remote service gateways often manage connections and credential authentication for these services.

Adversaries who have obtained valid account credentials may leverage external remote services as a point of initial access into your network and a mechanism for establishing persistence.

Detection Is A Challenge

Attacks from external remote services are difficult to detect given the use of valid credentials to obtain initial access. This gives the appearance of legitimate authentication to the services, therefore discovering the malicious activity before damage is done involves threat hunting expertise and advanced machine learning capabilities.

Suspicious Remote Access can be leveraged in every stage of the "Cyber Kill Chain", AKA attack path so vigilance in detecting adversary presence is key.



The Infosec Institute published an article that included three things to look out for when trying to detect Suspicious Remote Access²:

1. **Collect authentication logs:** Authentication logs might be able to indicate suspicious account activity. For instance, accounts might be detected logging in at odd hours or outside business hours. Multiple accounts that are logged into a system simultaneously can also indicate a red flag. Shared accounts (user, admin or service accounts) should also be monitored for suspicious activities.
2. **Conduct regular security tests:** Conducting pentests regularly might be able to identify malicious activity in progress. Pentests are able to uncover user accounts that may have been created by an adversary for persistence. Default accounts (such as Guest), credentials and SSH keys should be monitored and taken into account.
3. **Correlate security information:** It is important to correlate login information with other security information. For instance, a scenario where a user account session is observed to be active while the user has never had VPN access granted nor even entered the premises might indicate a red flag.

The eSentire Threat Response Unit (TRU) saw a need for an analytics tool that would detect suspicious behavior using valid credentials in order to deliver additional threat detection capabilities to customers of eSentire and they created Malkara.

What Is Malkara?

Malkara is a suspicious remote access analytic tool built by the eSentire TRU team. Malkara is built on top of eSentire's MDR for Log core functionality and is designed to detect situations where adversaries use valid account credentials to gain access to enterprise networks in order to obtain initial access and maintain persistence within a target environment. The initial scope of this analytic is remote VPN sessions and some cloud services, and it will expand to cover more in the future.

Malkara is a type of machine learning model called an autoencoder, a type of Artificial Neural Network (ANN) which has been trained using sample data. Autoencoders are an unsupervised learning technique common in the image recognition/classification space and are gaining popularity in the field of anomaly detection. Autoencoders work by taking input data and applying a trained dimensionality reduction algorithm in order to obtain a synthesized, compressed output representation of the original data. The autoencoder will then attempt to reconstruct input data from the output representation and calculate a fidelity score of the reconstructed input to determine how well the algorithm is performing. This fidelity score is known as reconstruction error; outliers will have a high reconstruction error.

Suspicious Remote Access Attack Detection Using MDR for Log And Malkara

Malkara inspects remote access sessions for anomalous activity. The model takes several data points into account to analyze and make inferences:

- Overlapping concurrent remote user sessions
- Time and distance vectors
- Remote connection type (examples: Cellular, Residential, Commercial, Government, Academic)
- Remote connection anonymization type (examples: VPN, Hosting Provider, Public Proxy, Tor Exit Node)
- Session time of day and duration
- Session bytes transmitted and received

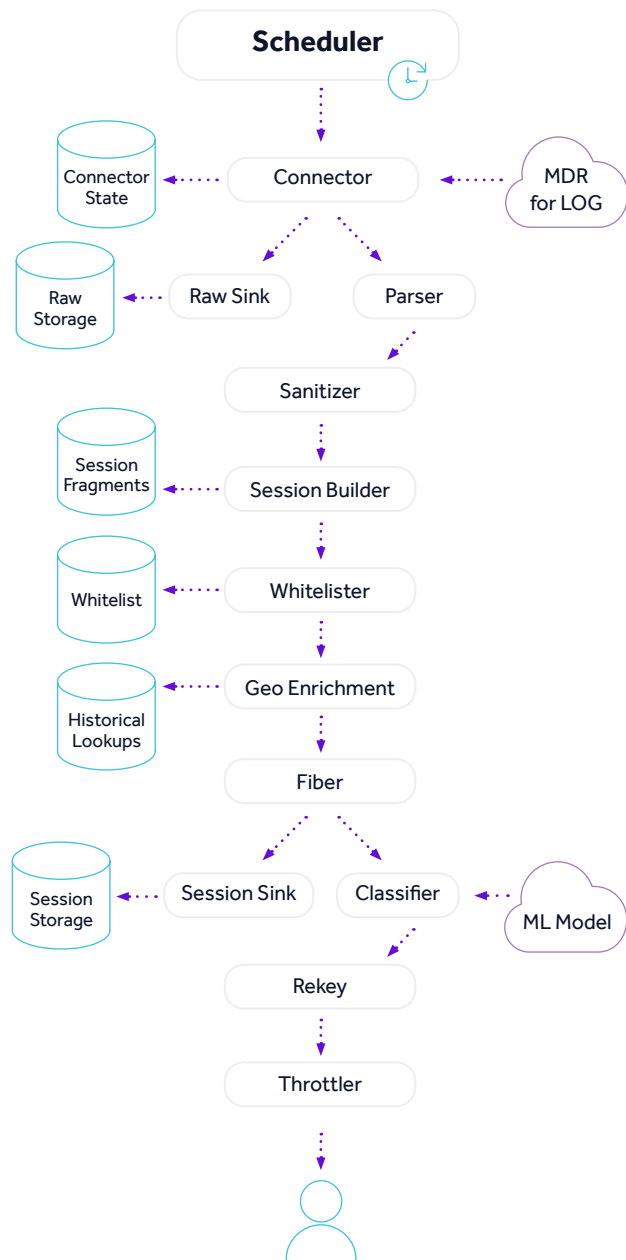
Using this information the model is able to find potential 'outliers' that deviate from the training data set which contains a large amount of 'good' sessions.

The main data source for Malkara is application logs from the different sources that Malkara services. All of those sources should be available through MDR for Log if the customer has the applications set up in their environments. Using application specific queries a data source needs to have the following fields to be enriched enough for the model to make meaningful predictions:

- Username
- Bytes Sent
- Ip Address
- Bytes Received
- Session Duration

If there are no durations available then, there needs to be a session start and a session end log so we can calculate a session duration so we can determine overlaps.

Malkara Architecture



1 <https://attack.mitre.org/techniques/T1133/>

2 <https://resources.infosecinstitute.com/mitre-attck-external-remote-services/>


Suspicious Remote Access Attack Containment using MDR for Log and Malkara

eSentire's global Security Operations Centers (SOCs) primarily detect and stop remote access attacks using MDR capabilities via MDR for Log and Malkara functionality. During the penetration testing engagement performed by one eSentire client, security consultants from a third party security provider successfully obtained valid account credentials through a phishing attack against a user. Once valid credentials were obtained, the security consultants were able to successfully authenticate against the client's VPN concentrator to gain initial access to the environment. During eSentire's investigation, log records associated with this incident were manually retrieved from the client's MDR for Log instance and processed through the Malkara pipeline. This session was scored as -0.685313 by the Malkara analytic. The suspicious decision boundary threshold is set at 0.55. Sessions below this score are deemed benign and sessions at or above this threshold are deemed suspicious.

Malkara would have flagged this session as suspicious and sent an alert to eSentire's eSentire's SOC to initiate an investigation.

Continuing the fight against attacks that hijack remote services

Utilizing the suspicious remote access analytic tool, Malkara, coupled with the data from MDR for Log, eSentire is able to detect situations where adversaries use valid account credentials to gain access to networks with malicious intent and stop them in their tracks, before they achieve their objective. As remote access VPN tools continue to be a popular attack vector for cybercriminals, Malkara continues to learn and enhance its detection capabilities. Combining machine learning with human expertise and applying it to eSentire's MDR capabilities, our SOC analysts are empowered to disrupt and contain threats like suspicious remote attacks every day.

If you're experiencing a security incident or breach contact us  1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit www.esentire.com and follow [@eSentire](https://twitter.com/eSentire).