**IR Book – Malicious Remote Access Alert**

**Introduction**

The Incident Response (IR) plan is an important part of risk management. Preventative security controls based on the results of risk assessments can reduce the number of incidents, but not all incidents can be prevented. When incidents cannot be prevented, preemptive measures in addition to security controls can reduce the potential impact, and shorten the time required for complete remediation.

Malware can potentially have different effects on the production network:

**Safety** – it can alter production parameters to degrade operational safety

**MBMO**

**INCIDENT RESPONSE PLAYBOOK**

**MALICIOUS REMOTE ACCESS ALERT**

**Productivity** – it can reduce production quality and/or quantity

**Reliability** – it can cause production system to behave erratically. In the automotive industry, reduced quality can also effect passenger safety.

An incident response capability is therefore necessary for prompt detection of incidents, containment of the affected area in order to minimize losses and safety (destruction), mitigation of the weaknesses (breaches or vulnerabilities) that were exploited, and to quickly restore productivity and reliability.

This playbook provides guidelines for incident handling in the Mercedes Benz production shop floor, and in particular, to analyze incident-related data in order to determine the most appropriate response.

**Definition of malicious remote access**

Malicious remote access is a situation in which an attacker manages to leverage the organization’s remote access solution to penetrate the shop floor network, take control over engineering stations, HMI ,or controllers, and disrupt production.

The attacker intentions can vary from monetary gain (e.g., ransomware as a tool to make management pay, or cryptoware to utilize computer resources) to targeted attacks designed to cripple the plant’s production processes.

A successful remote access breach usually does not need to install additional tools to control the infected station, since the attacker is using a legitimate channel to manage an asset.

This makes the attack very hard to detect with customary security tools, due to lack of signs or anomalies in the attacked assets.

There are several methods of attack that originate in the remote access solution.

The following table describes the different categories.

|  |  |
| --- | --- |
| Category | Description |
| Infected computer | An approved client computer is controlled by an attacker. Using the existing access to the shop floor, the attacker can manipulate the asset through the infected computer. From the security team perspective, there is nothing out of the ordinary. |
| Stolen credentials | Through an early reconnaissance, the attacker manages to acquire legitimate user credentials for remote access. Using these credentials, the attacker can access the network freely. |
| Remote access gateway vulnerability | Utilizing a zero-day exploit, the attacker manages to attack the remote access gateway, and to obtain a legitimate user token to access the network. |
| Remote access security misconfiguration | Deploying the remote access gateway without proper security hardening, provides an attacker with the opportunities to take advantage, to access the gateway in a legitimate way. |
| Man-in-the-Middle | Using communication manipulation between the client and the remote access gateway, the attacker manages to eavesdrop and manipulate the network traffic between them to his advantage. |
| Denial of Service | Less of a breach, but designed to interrupt remote operations, the attacker manages to take down the remote access service. |

**Incident Response Phases**

IR can be a complicated process if the attacker does not need to download and install specialized tools, but instead uses legitimate access. Unless your plant has an experienced IR team, it is recommended to reach out and get outside help in these cases.

There are six principal phases for the incident response process:

**Prepare**

The need to execute an [incident response](https://www.fireeye.com/services/mandiant-incident-response.html) (IR) procedure can occur at any time, and there are many steps that an organization can take to be prepared. These preparation steps can empower an organization to enhance its ability to detect a potential incident faster, rather than being notified by an external entity that an incident has possibly occurred.

When an incident occurs, and an incident response is initiated, the success and accuracy of the investigation depends on having complete and consistent visibility for all systems and network communication paths throughout the enterprise environment.

These points represent practical steps that all organizations can take ahead of time to minimize the number of roadblocks and delays that could impact the success of an investigation:

This stage is everyone’s responsibility, from the 1st tier analysts through to the plant BISO. Each role should have all relevant information ready.

Prepare for this by creating the data base described below, and updating it every six months.

(The more detailed and accessible the information you collect is, the faster and more accurate the triage and subsequent stages will be. This will ultimately lead to a more efficient incident recovery, and to lower production downtime and losses)

|  |  |
| --- | --- |
| **Process** | 1. Contact information:  Prepare a table with the plant network/security and relevant managers details, including exact position, responsibility, email addresses and 24/7 telephone numbers. Make sure the table is accessible to all IR relevant teams.  2. Investigation record tool:  Pick an easy to use software tool that supports: multiple party interaction, search engine and history collection. Make sure every active member in the IR procedure is familiar with how to use the tool.  3. Asset inventory list:  Create and update on a regular basis a detailed list of the shop floor’s assets, including enterprise-related assets (directly connected to the production, such as: DMZ, ERP, etc.). Ensure all the assets directly connected to the remote access gateway are inventoried.  4. Network:  Prepare a table with all remote access solution routing rules to shop floor assets (both from the remote gateway configuration, and the relevant firewall rules).  Collect all network topology and architecture documents, including all segmentation and ACL information.    5. Credentials:  Maintain an accurate inventory of all remote access users, including administrator accounts.  6. Logging:  Verify that detailed logging is present for every remote access connection, including as minimum: source and destination IP addresses, ports, and duration.  For endpoints, verify that log data exists to support a review of:   * + Successful and failed logon events   + System events   + Scheduled tasks   + Process execution events with command line arguments   + Security software events (e.g.: third-party Antivirus alerts and detections)     7. Recovery repository:  Make images for shop floor assets. Keep them in a secure segment, and limit access to it. Beside using them to quickly recover from loss, they can be used as a clean baseline to analyze infected assets.  8. Verify changes every 6 months:  Verify and validate all gathered information is updated, go over each section and update as necessary. |

A prerequisite for the IR process is to ensure that all potential detection tools and all human observations are channeled to the same team (aka SOC).

**Identify**

The Identification stage deals with the identification and initial scoping to detect whether the network has been breached through the remote access solution.

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.

Identifying possible remote access breaches can be done in the following ways:

**A close up of a logo

Description generated with very high confidence**A close up of a logo

Description generated with very high confidenceA close up of a logo

Description generated with very high confidence **Sight -** the hardest to detect, it depends on two crucial factors:

1. attack progression and asset manipulation can be observed directly on the asset screen (e.g., mouse movements or keyboard typing without human intervention).

2) security-aware personnel, who see the action and raise an alert to the relevant team.

**Outcome** - the attack’s effect on production are noticeable by either an operator or some controller’s software: for example, the machine slows production without apparent causes, or an HMI’s resource use suddenly goes very high (CPU, memory etc..).

**Monitoring –** The shop floor security log and network traffic analysis tool raises an alert due to suspicious activity in the network or on a computer (e.g., a new protocol used on the shop floor network, or an unrecognized process starting in an unusual way on a computer).

The identification stage is handled by the production network/security team.

|  |  |
| --- | --- |
| **Relevant tools** | Sophos  Bomgar/Netop  Host operating system logs  Active Directory logs  Asset inventory list  Incident management tool |
| **Process** | 1. Initial Alert:  a malicious remote access alert is generated by one of the shop floor’s cyber-security monitoring tools (e.g., AV, log management system, etc.), or a production anomaly is encountered. A malware alert could also be initiated manually by the shop floor operators observing an anomalous behavior. The notification will usually follow unexplained activity on an engineering station, HMI, or PLC.  2. Create an Investigation Record.  An investigation record is opened for each discrete alert, within the incident management tool, and relevant investigative data is recorded. Duplicate events can be aggregated to a previously opened case, provided the investigation record is still in the opened state. The cases should be accessible to any SOC, BISO team, or IR team member, and easily retrieved.  3. Gather the following information regarding the remote access from the Bomgar/Netop logs. If there are several potential malicious connections, collect the information for all of them:  - Time of connection  - User name  - Length of connection  - User source IP  - User destination IPs  Add the information to the case record.  4. Asset summary  Gather the following information about the manipulated hosts:  - Hostname  - OS version  - Asset functionality  Add the information to the case record.  5. Affected User summary  Collect details about the affected user (the one used by attacker) from Active Directory:  - User ID  - User’s name, title, department, physical location  Add the information to the case record. |



As in any other activity – “practice makes perfect”. Try to simulate, locally or

externally with 3rd parties, incidents. Train your SOC and IR people on a regular basis.

Evaluate performance and use feedback to improve.

**Triage**

The Triage stage deals with verifying whether the security alert is, in fact, an incident, determining the severity of the incident, and performing additional analyses.

This operations in this stage are handled by the 1st level incident response team.

|  |  |
| --- | --- |
| **Relevant tools** | Contact list  Asset inventory list  Incident management tool |
| **Process** | 1. As long as there is no production impact, proceed meticulously at this stage. Whenever there is a risk of a production disruption, quickly move to the Investigate or Remediate stage, according to the severity of the impact.  2. Contact the asset owner and the network team, to confirm the changes or consequences were not caused by them.  3. Perform an impact analysis (table 2) to prioritize asset remediations and to determine the level of notification escalation.  4. If the unexplained asset behavior appears on several computers during a short period of time (several minutes), or it drastically effects the  safety/productivity/reliability of the shop floor, escalate the incident  into the highest impact level, and start REMEDIATE steps, in parallel with INVESTIGATE steps, immediately. |

**Start documenting timestamps for every action performed from this point on**.

Determine the potential impact using the following calculation:

Table 1 – Infection effect

|  |  |
| --- | --- |
| Low | No loss of visibility or control on all level devices |
| Medium | Some Loss of visibility on level 02 or 03 assets, no disruption to manufacturing |
| High | Loss of visibility and control on level 02 and 01 assets |

Table 2- Potential damage

|  |  |
| --- | --- |
| Low | Infected host/s does not handle any process control |
| Medium | Infected host/s handles a minor-importance process control |
| High | Infected host handles major- or several minor-importance process controls |

Notify appropriate individuals about incident details, according to the following table:

|  |  |  |
| --- | --- | --- |
| **Effect** | **Damage** | **Role to notify** |
| Low or Medium | Low | SOC Team leader |
| Low or Medium | Medium | Security manager + tier 2 IR team |
| High | medium | IT manager |
| High | High | COO |

Update the case record with all activities.

**Investigate**

The Investigation stage deals with the security incident in detail, ensuring that all  
information is documented. By the end of this stage you will have the full scope of the incident.

This stage is handled by an incident response trained team, with IR tools such as Sophos X intercept, Redline, or other open source or commercial tools.

Pay attention (and review the Malicious Malware Playbook, particularly the Identify stage) to any malware the attacker might have downloaded and installed on the remotely controlled hosts. If such activities are identified, execute the “malicious malware” playbook simultaneously.

It is highly discouraged to skip the Investigate phase, and go directly to Remediate since discovery of the attacker’s point of entrance into the network is crucial to remove or block any future breach attempts.

The only exception to this is when the effect of the breach on the shop floor is drastically disrupting production. In this case Remediation is done as an emergency procedure (described in Remediation stage) and might require shutting down assets indiscriminately.

|  |  |
| --- | --- |
| **Relevant tools** | Sophos intercept/Redline (hosts forensic tool)  Firewall logs  Hosts operations systems logs  Bomgar/Netop connection logs  Incident management tool |
| **Process** | 1. Review the information that is available, and ensure that an  accurate collection of the IOCs for this breach have been  thoroughly collected.  2. Look in Bomgar/Netop logs and write down any active user sessions for the relevant time period (starting with the initial identify stage time), and look in Active Directory (or OS hosts logs) for additional activity by these users in that time period. Add any hosts/assets that were logged into by those users to the infected host lists.  3. Look in Bomgar/Netop and FW logs (pay attention to the relevant  TIMESTAMP) for the IP of affected hosts, find unfamiliar communications from infected hosts to “clean” hosts. Add the “clean” host to the infected host list  4. Explore infected hosts Operation systems logs, focusing on logging logs  . Look for unfamiliar processes, created/modified files, created/modified registry keys. Add the hosts with unusual activity to the infected hosts list.  4. Repeat the “determine the potential impact” step of the previous stage  (TRIAGE) and escalate notification appropriately. |

 Install and learn how to use the Redline free open source tool from FireEye.

This tool can be used for deep investigation of end points. It is very extensive and very

useful.

At the end of the process you should be able to answer the following questions:

1. How did the attacker initially penetrate your system?
2. What credentials is the attacker using?
3. Which hosts did the attacker manipulate?

Update the case record with all activities and insights.

**Remediate**

This stage deals with the containment and removal of the remote attacker from your environment.

Containment aims to stop the offensive operations of the remote attacker in the network, while removal prevents the attacker from coming back through the original penetration vector.

This stage is handled by the network/security team together with the IR team.

Proper containment disconnects the attacker from the remote connection and the shop floor network, and allows gradual and unstressed production recovery. If, after disconnecting the remote access connection, there is still suspicious unexplained activity in the network, refer to the “malicious malware” playbook for further actions.

|  |  |
| --- | --- |
| **Relevant tools** | Sophos intercept / Redline  Check Point firewall  Bomgar/Netop  Incident management tool |
| **Process** | Containment:  1. Disconnect the attacker session through the Bomgar/Netop gateway, and block any new connection through the remote access gateway until the end of Remediate stage.  2. Restart infected hosts (recognized in the previous stage). If proper functionality of the host is missing due to sabotage, re-image the host.  3. If the breach originated from an infected authorized client computer, block further connection from this device until proper application of security countermeasures has been applied to that computer.  4. If the breach was due to some gateway vulnerability or misconfiguration, disconnect the remote access gateway until the problem has been resolved (i.e., patching or hardening).  **Apply containment procedures to all compromised hosts at the same time.**  Removal is an immediate or parallel step to containment:  1. Reset all fixed remote access passwords including the administrator password  2. Validate existing users in Bomgar/Netop against the credentials list from the Prepare stage. Delete any unexplained user.  3. Update the Investigation Record with all actions performed. |
|  |  |
| **Emergency procedures** | 1. Disconnect all remote access sessions on Bomgar/Netop  2. Quarantine (disconnect from network), if possible, or shutdown infected  hosts  3. Perform the “malicious malware” Investigate stage for the quarantined hosts, to detect any installed malicious tools.  4. To resume production quickly, use re-imaging with formatting.  5. Do not forget to save infected images for later investigation.  6. Update the Investigation Record with all actions performed . |



There are pros and cons to each decision. A full and extensive investigation would likely reveal more about the initial infection and its spread throughout the network, the entire suit of tools, and the source of attack. But, delaying the removal of the attacker might cause severe damage to the plant. Either way, this decision should be approved by upper management.

After a successful removal, keep a close watch for the next 24 hours, and carefully investigate any unusual alert on one of the infected hosts, or any suspicious remote connection.

Update the case record with all activities.

**Post-Incident**

The Post-Incident stage concludes the incident investigation, ensuring that everything was thoroughly checked. The incident case can be closed once the investigation is completed.

This stage also serves as a learning and improvement phase. In accordance with the incident complexity and severity, initiate a comprehensive debriefing.

This debriefing will make sure the you have answers to these questions:

⏹Exactly what happened, and at what times?  
⏹ How well did staff and management perform in dealing with the incident? Were the

documented procedures followed? Were they adequate?  
⏹ What information was needed sooner?  
⏹ Were any steps or actions taken that might have inhibited the recovery?  
⏹ What would the staff and management do differently the next time a similar incident

occurs?  
⏹ What corrective actions could prevent similar incidents in the future?  
⏹ What additional tools or resources are needed to detect, analyze, and mitigate future

incidents?

This stage should also serve as an trigger to enhance the cyber-resiliency of the shopfloor.

Some recommendations that could result from this stage:

- lower response time (and potential damage) by improving cyber security policies and network/systems hardening

- acquire additional security tools, missing backup and restore tools, and this playbook’s additional drilldown guidelines

- perform advanced team training



Use the opportunity to re-evaluate the remote access solution security measures. Could prevention and detection tools be improved? Rethink alternate deployments. Schedule a red-team assessment of your current solution.

**Stay Safe**