

Incident Response Guide

Effective Date: 1-JUNE-2021
Last Updated: FEBRUARY-2024

Contents

Introduction	2
Partnership	2
Areas of Responsibility	3
Detections	4
Cyber Threat Intelligence	5
Event Data Collection, Analysis and Triage (DETECT)	6
Incident Response (RESPOND)	8
Remediation (RESPOND)	12
Recommended Mitigations	13
Conclusion	14

Introduction

RocketCyber SOC team works on the IT PARTNER's behalf to detect, respond, and remediate critical cybersecurity incidents via all tools and methods available. The arsenal of the RocketCyber's incident response team is constantly adapting to global threat patterns by developing new apps and integrations that blend machine and human learning & actions. The combined automated and manual approach provides a redundant layer of action to effectively detect, investigate, contain, report, and recover.

We base our incident response model on the National Institute of Standards and Technology ([NIST](#)) Framework of Improving Critical Infrastructure Cybersecurity and the [MITRE ATT&CK](#)[®] Framework, among others. The frameworks enable organizations to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. It provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.

Partnership

RocketCyber's success depends heavily on close collaboration with the IT Partner and their ability to implement the strictest security measures possible. RocketCyber will constantly advise its Partners to fortify their networks defenses against cyber threats via the following methods:

- Deploy and maintain next generation endpoint protection.
- Implement strict firewall policies at the network edge.
- Train employees to be vigilant.
- Activate MFA for all admin and user accounts.
- Frequently backup and use continuous data protection software.
- Practice a least-privilege approach.
- Implement a plan for continuous operations.
- Always install system updates.

Areas of Responsibility

Based on the NIST model we summarize the areas below that depict responsibilities of RocketCyber and the IT PARTNER to ensure the most effective ability to DETECT, RESPOND, and RECOVER to a cyber event.

FUNCTION	RESPONSIBILITY	CATEGORY
IDENTIFY	IT PARTNER	Asset Management
	IT PARTNER	Business Environment
	IT PARTNER	Governance
	IT PARTNER	Risk Assessment
	IT PARTNER	Risk Management Strategy
	IT PARTNER	Supply Chain Risk Management
PROTECT	IT PARTNER	Identity Management, Authentication & Access Control
	IT PARTNER	Awareness and Training
	IT PARTNER	Data Security
	IT PARTNER	Information Protection Processes and Procedures
	IT PARTNER	Maintenance
	IT PARTNER	Protective Technology
DETECT	RocketCyber SOC	Anomalies and Events
	RocketCyber SOC	Security Continuous Monitoring
	RocketCyber SOC	Detection Processes
RESPOND	RocketCyber SOC	Response Planning
	RocketCyber SOC	Communications
	RocketCyber SOC	Analysis
	RocketCyber SOC	Mitigation (Device Isolation)
	IT PARTNER	Mitigation/Remediation
	RocketCyber SOC	Improvements
	IT PARTNER	Improvements
RECOVER	IT PARTNER	Recovery Planning
	IT PARTNER	Improvements
	IT PARTNER	Communications

Detections

A threat event has the potential for causing consequences or impact. Events include unauthorized access to computers, unauthorized use of system privileges and execution of malware that destroys, encrypts a system, or steals data. Think of an event as an observable occurrence, such as when a failed login to a computer occurs. While this could be either unintentional or intentional, both are considered events.

A security incident is a violation or imminent threat of security policies or industry best practices. Incident examples include:

- Denial of service – an attacker sends high volumes of connection requests to a server, resulting in a crash.
- Phishing – employees are enticed to click and open EMAIL/PSA attachments or links resulting in malware deployment or establishing a connection with external systems.
- Malware – Type of application designed to perform a variety of malicious tasks: create persistent access, spy on the user, create disruption, etc. The most notable form of Malware is Ransomware.
- Ransomware – an attacker obtains unauthorized access, encrypting the system and asking for a financial sum of money before the computer is decrypted and operational.
- RDP hijacking - involves the attacker “resuming” a previously disconnected RDP session. This allows the attacker to get into a privileged system without having to steal the user’s credentials.
- PowerShell - Attackers commonly use command and script interpreters such as PowerShell to execute malicious commands, run scripts, and binaries when carrying out an attack.
- PowerShell without PowerShell – PowerShell commands and scripts can be executed by loading the underlying System.Management.Automation namespace. As a result, this eliminates the need to spawn powershell.exe.
- Business EMAIL/PSA Compromise (BEC) – an attacker has gained unauthorized access to an employee’s EMAIL/PSA.
- Man-in-the-middle attack (MITM) – attacker intercepts the communication between two parties to spy on the victims, steal personal information or credentials, or alter the conversation in some way.
- Zero-day exploit – Cyber-criminals learn of a vulnerability that has been discovered in certain widely-used software applications and operating systems, and then target organizations who are using that software to exploit the vulnerability before a fix becomes available.
- Cryptojacking – Cyber criminals compromise a user’s computer or device and use it to mine cryptocurrencies, such as Bitcoin.
- DNS Tunnelling – Is a sophisticated attack vector that is designed to provide attackers with persistent access to a given target. Since many organizations fail to monitor DNS traffic for malicious activity, attackers can insert malware into DNS queries (DNS requests sent from the client to the server). The malware is used to create a persistent communication channel that most firewalls are unable to detect.
- Drive-by Attack – A ‘drive-by-download’ attack is where an unsuspecting victim visits a website which in turn infects their device with malware. The website in question could be one that is directly controlled by the attacker, or one that has been compromised. In some cases, malware is served in content such as banners and advertisements. These days exploit kits are available which allow novice hackers to easily set up malicious websites or distribute malicious content through other means.
- Eavesdropping attack – Sometimes referred to as “snooping” or “sniffing”, an eavesdropping attack is where the attacker looks for unsecured network communications to intercept and access data that is being sent across the network. This is one of the reasons why employees are asked to use a VPN when accessing the company network from an unsecured public Wi-Fi hotspot.

Cyber Threat Intelligence

One of the approaches we follow is MITRE ATT&CK Mapping to help us understand adversary behavior as a first step in protecting networks and data. The MITRE ATT&CK® framework is based on real-world observations and provides details on 100+ threat actor groups, including the techniques and software they use. It helps identify defensive gaps, assess security tool capabilities, organize detections, hunt for threats, or validate mitigation controls.

ATT&CK describes behaviors across the adversary lifecycle, commonly known as tactics, techniques, and procedures (TTPs). These behaviors correspond to four increasingly granular levels:

- Tactics represent the “what” and “why” of an ATT&CK technique or sub-technique. They are the adversary’s technical goals, the reason for performing an action, and what they are trying to achieve. For example, an adversary may want to achieve credential access to gain access to a target network. Each tactic contains an array of techniques that network defenders have observed being used in the wild by threat actors.
- Techniques represent how an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access. Techniques may also represent what an adversary gains by performing an action. A technique is a specific behavior to achieve a goal and is often a single step in a string of activities intended to complete the adversary’s overall mission.
- Sub-techniques provide more granular descriptions of techniques. For example, there are behaviors under the OS Credential Dumping technique that describe specific methods to perform the technique. Sub-techniques are often, but not always, operating system or platform specific. Not all techniques have sub-techniques.
- Procedures - how a technique or sub-technique has been used. They can be useful for replication of an incident with adversary emulation and for specifics on how to detect that instance in use.

The steps we follow are:

- Find the behavior. Searching for signs of adversary behavior is a paradigm shift from looking for Indicators of Compromise (IOCs), hashes of malware files, URLs, domain names, and other artifacts of previous compromise. The RocketCyber Agent is collecting signs of how the adversary interacted with specific platforms and applications to find a chain of anomalous or suspicious behavior prior to damage to the customers’ businesses.
- Research the Behavior. Additional research may be needed to gain the required context to understand suspicious adversary or software behaviors. Use additional resources integrated with RocketCyber’s platform and/or external resources when needed, to gain information on the potential threat.
- Identify the Tactics. Comb through the report to identify the adversary tactics and the flow of the attack. To identify the tactics, we focus on what the adversary was trying to accomplish and why. Was the goal to steal the data? Was it to destroy the data? Was it to escalate privileges?
- Identify the Techniques. After identifying the tactics, review the technical details associated with how the adversary tried to achieve their goals. For example, how did the adversary gain the Initial Access foothold? Was it through spear-phishing or through an external remote service? Drill down on the range of possible techniques by reviewing the observed behaviors in the report.
- Identify the Sub-techniques. Review sub-technique descriptions to see if they match the information in the report. Does one of them align? If so, this is probably the right sub-technique. Depending upon the level of detail in the reporting, it may not be possible to identify the sub-technique in all cases. Read the sub-technique descriptions carefully to understand the differences between them. For example, Brute Force includes four sub-techniques: Password Guessing, Password Cracking, Password Spraying, and Credential Stuffing.
- Take or recommend remediation steps depending on the identified threat(s).

Event Data Collection, Analysis and Triage (DETECT)

Triage is the investigation of a threat event, resulting in a verdict of malicious, suspicious, or benign. Events defined as malicious or suspicious are considered an incident. Events are generated throughout the day and span networks, endpoints (computers) and cloud applications.

The RocketCyber SOC utilizes multiple cyber intelligence feeds that help enhance many of the services below to detect new emerging threats. The RocketCyber agent provides continuous monitoring for suspicious or malicious behavior and presents these findings in data that can be actioned through automation or human analysts.

Below is a list of ever evolving services that the RocketCyber Platform and SOC team are constantly monitoring, triaging, and responding to. Should a serious threat be found, the RocketCyber agent can isolate the device from the rest of the network. This allows further investigations without exposing threats to the rest of the customer systems.

APP	DETECT
ADVANCED BREACH DETECTION	The RocketCyber Agent identifies computers that are compromised where security defenses have been circumvented. Malicious activity reported by our SOC agent requires immediate investigation.
CRYPTO MINING DETECTION	The RocketCyber Agent detects crypto mining activity from browser based crypto miners as well as common crypto mining client software.
CYBER TERRORIST NETWORK CONNECTIONS	The RocketCyber Agent detects network connections to various nation states that have been known to engage in cyberterrorist activities and malicious network activity such as backdoor connections to C2 servers and malicious systems.
DATTO EDR MONITOR	This app receives events from Datto EDR.
DNS FILTER MONITOR	Collects information from DNS Filter.
ENDPOINT EVENT LOG MONITOR	The RocketCyber Agent monitors the Microsoft Windows or macOS Event Log for suspicious events. Detected events are security related activities such as failed logins, clearing security logs, unauthorized activity, etc.
FIREWALL LOG ANALYZER	The RocketCyber Agent acts as a syslog server collecting log messages from edge devices on your network. Messages are parsed and analyzed for potential threat indicators. When a potential threat or security related event is detected, it will forward the detection to the Cloud Console.
GRAPHUS	This app will collect alerts from Graphus EMAIL/PSA Security

IOC DETECTION	Continuous monitoring for Indicators of Compromise to address emerging and changing threats
MALICIOUS FILE DETECTION	The RocketCyber Agent monitors and detects suspicious and malicious files that are written to disk or executed.
MICROSOFT EXCHANGE THREAT DETECTION	This app will look for specific IOC's related to exploitation of Microsoft Exchange
OFFICE 365 LOGIN ANALYZER	Detects logins outside the expected countries or known malicious IP addresses
OFFICE 365 LOG MONITOR	The SOC Platform ingests and reports on Microsoft Office 365 and Azure log data.
OFFICE 365 RISK DETECTION	We focus on the riskiest accounts, users, and behaviors. Determined risk through a combination of industry heuristics and machine learning.
OFFICE 365 SECURE SCORE	Overall description of cloud security posture with itemized remediation plans across all Office365 tenants.
SUSPICIOUS NETWORK SERVICES	The RocketCyber Agent detects suspicious network services running on an endpoint. While there are 65,535 available network services for legitimate use, suspicious detections are defined as well-known ports and services that are leveraged for malicious intent.
SUSPICIOUS TOOLS	The RocketCyber Agent detects programs that can negatively impact the security of the system and business network. Detected suspicious tools should be investigated and are categorized as hacking utilities, password crackers, or other tools used by attackers for malicious purposes.
ACTIVE DIRECTORY MONITOR AND SYNC	This app will monitor for changes to user accounts in Active Directory and synchronize changes to the Breach Secure Now Cloud. Optionally reporting changes to the Console.
BITDEFENDER	The SOC Platform ingests and reports on detections from BitDefender.
DEFENDER	The SOC Platform ingests and reports on detections from Defender.
DEFENDER FOR BUSINESS	The SOC Platform ingests and reports information from Defender for Business.
CYLANCE	The SOC Platform ingests and reports on detections from Cylance.
DEEP INSTINCT	The SOC Platform ingests and collects information from Deep Instinct.
SENTINELONE	The SOC Platform ingests and reports on detections from SentinelOne.
SOPHOS	The SOC Platform ingests and reports on detections from Sophos.
WEBROOT	The SOC Platform ingests and reports on detections from Webroot.

Incident Response (RESPOND)

The threat landscape and attacker’s techniques are constantly evolving. While it is not feasible to list every attack and response scenario, the tables below outline common attack techniques and the anticipated actions of the RocketCyber SOC team and the IT Partner. While the list is not exhaustive, please use this as a guideline of what to expect when incidents are detected via the RocketCyber SOC platform.

When calling, the SOC will call all available numbers in the Notifications section. If a critical threat to a business system is detected, the SOC will disconnect the device from network to stop the spread of the threat even in the event when no one can be reached, unless otherwise specified by the IT Partner in the Notifications Tab > Special Instructions field.

Upon generation of an Incident (PSA ticket or Email Notification), the RocketCyber SOC team will determine if the event qualifies as an Indicator of Compromise (IOC).

Please note that:

- If the event(s) indicate critical IOC(s), the SOC will further escalate the incident by calling the Partner and isolating device(s). For every situation that requires isolation, the SOC will create a ticket to enable 2-way communication between the Partner contacts in the Permissions Tab and the SOC.
- After the initial IOCs were detected, the analysts will conduct an in-depth investigation to look for any other unusual events (we do not recommend archiving of events as they auto-archive on their own every 35 days).
- Based on what it finds, the SOC will isolate the device(s) if:
 - The provider does not answer the call to confirm action(s) are authorized.
 - The SOC cannot determine with 100% certainty that any stages of an attack are not in progress based on the incidents and events found in the customer’s dashboard at the time.
- The Apps serve as event collectors; the SOC triages the data in the apps to identify any unusual activity that might require further investigation. If events of interest are discovered and action by the Partner will be required, a logic rule will be created to generate notifications automatically.
- The SOC factors the time-zone for the business and after-hours executions in the decision-making process.
- We strongly recommend that the RocketCyber agent be installed on all devices – servers, local computers, and remote computers used for remote access.

SEVERITY LEVELS – EVENTS / INCIDENTS







Severity	Impact	Description	Typical Response Detection/Incident/Action	SLA
SEV 1	Critical-Urgent	Attack in progress. One or multiple devices show signs of compromise. AV detected ransomware, worm, backdoor, hacktool utilities, etc.	2min / 5min / 10min	10 Minutes
SEV 1	Critical	RocketCyber/Datto EDR detected malicious, suspicious, unusual process executions, files, or connections.	2min / 5min / 10min	15 Minutes
SEV 2	Major	Low-level detections with a VirusTotal score >9.	2min / 10min / As Needed	60 Minutes
SEV 3	Minor	Low-level detections with a VirusTotal score <10.	2min / 10min / As Needed	N/A
SEV 4	Info	No malicious effect on the system is observed.	2min / As Needed / As Needed	N/A



CYBER TERRORIST NETWORK CONNECTIONS				
DETECT	ANALYZE	REMIEDIATION / MITIGATION		ACTIONS
RocketCyber	RocketCyber	RocketCyber	IT PARTNER	RocketCyber
Suspicious RDP Connection	Analyze details. Review timeline. Identify other suspicious events.	If successful login detected, notify IT Partner. Critical - If unauthorized, isolate device .	If unauthorized, change all user passwords with access to device. Run a full AV scan. Investigate root cause. Apply strict access policies.	EMAIL/PSA CALL ISOLATE
		If brute force detected but no successful login detected, notify IT Partner.	Place RDP behind VPN. Update system. Apply strict access policies.	EMAIL/PSA
Suspicious SQL Connection	Analyze details. Review timeline. Identify other suspicious events.	Critical - If the connection is successful, notify IT Partner. If unauthorized, isolate device .	If unauthorized, change all user passwords with access to the device. Run a full AV scan. Apply strict access policies.	EMAIL/PSA CALL ISOLATE
		If the connection is authorized, notify IT Partner.	Run a full AV scan. Apply strict access policies.	EMAIL/PSA CALL
Suspicious Inbound Connections on 445 or 25 (SMB/SAMBA/Windows File Sharing) or 139 NetBIOS Session Service	Analyze details. Review timeline. Identify any other suspicious events.	Critical - If the connection is successful, notify the IT Partner. If unauthorized, isolate device .	If unauthorized, change all user passwords with access to the device. Run a full AV scan. Investigate the root cause of compromise. Apply strict access policies.	EMAIL/PSA CALL ISOLATE
		If the connection is authorized, notify IT Partner.	If the Partner answers our call and confirms authorized, or current incident or previous incidents are resolved prior to the call the SOC will not isolate the device.	EMAIL/PSA CALL





DATTO EDR				
DETECT	ANALYZE	REMIEDIATION / MITIGATION		ACTIONS
RocketCyber	RocketCyber	RocketCyber	IT PARTNER	RocketCyber
Datto EDR -Host Isolation -Disable Service -Delete File -Terminate Process (DRMM can access device when isolated with DEDR)	Analyze details of threat (command line, file reputation). Review timeline. Identify any other suspicious events.	Critical - Isolate device and notify IT Partner.	If unauthorized, reimage the device(s), reset password for admin accounts. Work with the SOC to identify other IOCs.	EMAIL/PSA CALL ISOLATE
		Major - Isolate device or Delete file with Partner's approval.	If the file is unauthorized, restore device from a known good image or optionally, remove the file manually, and run a full AV scan. If the file is authorized, suppress alerts.	EMAIL/PSA CALL ISOLATE DEL FILE
		Medium – With Partner's permission, Delete File .	If the file is unauthorized, remove the file manually, and run a full AV scan. If the file is authorized, suppress alerts.	EMAIL/PSA CALL DEL FILE
AV MONITOR				
DETECT	ANALYZE	REMIEDIATION / MITIGATION		ACTIONS




RocketCyber	RocketCyber	RocketCyber	IT PARTNER	RocketCyber
SentinelOne Bitdefender Defender Defender for Business Cylance Webroot Sophos Deep Instinct	Analyze details. Review timeline. Identify any other suspicious events.	If threat is known malicious and not mitigated, isolate device , and notify IT Partner.	It is recommended to recover the system from a previous good image. Update signatures and run a full AV scan of the system.	EMAIL/PSA CALL ISOLATE
		If hash flagged as malicious, and not mitigated, notify IT Partner. Depending on details, isolate device .	If not authorized, It is recommended to recover the system from a previous good image. Update signatures and run a full AV scan of the system.	EMAIL/PSA CALL ISOLATE
		If threat mitigated, notify IT Partner.	Review the detection. Run a full AV scan of the system. Identify source of threat.	EMAIL/PSA
		If threat is a false positive or benign detection, notify IT Partner.	Suppress if appropriate.	EMAIL/PSA



ADVANCED BREACH DETECTION				
DETECT	ANALYZE	REMEDIAION / MITIGATION		ACTIONS
RocketCyber	RocketCyber SOC	RocketCyber SOC	IT PARTNER	RocketCyber
Suspicious Signed Binary Proxy Execution: -Regsvr32.exe -Mshta.exe -Msiexec.exe -Rundll32.exe	Analyze details. Review timeline. Identify any other suspicious events.	If malicious, notify IT Partner. Isolate device.	If not authorized, change passwords for users with access to device. Investigate root cause; depending on outcome, reimage.	EMAIL/PSA CALL ISOLATE
		If suspicious, notify IT Partner.	If not authorized, change passwords for users with access to device. Investigate root cause; depending on outcome, reimage. If authorized, resolve the incident. Apply incident suppression.	EMAIL/PSA CALL
Suspicious Download via PowerShell	Analyze details. Review timeline. Identify other suspicious events or incidents.	If malicious, notify IT Partner, isolate device .	If not authorized, change passwords for users with access to device. Investigate root cause; depending on outcome, reimage.	EMAIL/PSA CALL ISOLATE
Windows Firewall Disabled	Analyze details. Review timeline. Identify other suspicious events or incidents.	If malicious, notify IT Partner, isolate device .	If not authorized, change passwords for users with access to device. Investigate root cause; depending on outcome, reimage.	EMAIL/PSA CALL ISOLATE
Log Clears -PowerShell -Windows -Event Log	Analyze details. Review timeline. Identify any other suspicious events.	Notify IT Partner. isolate device if there are other IOCs and the IT Partner did not answer the call.	If not authorized, change passwords for users with access to device. Investigate root cause; depending on outcome, reimage.	EMAIL/PSA CALL
Suspicious Account Creation	Analyze details. Review timeline. Identify any other suspicious events.	Notify IT Partner. If unauthorized/Partner not reachable outside after hours, isolate device .	If not authorized, the device is compromised; remove the new account(s), change all user passwords with access to device.	EMAIL/PSA CALL ISOLATE
Suspicious Account Manipulation	Analyze details. Review timeline.	Notify IT Partner. If unauthorized/Partner not reachable, isolate device .	Run a full AV scan. Investigate root cause and depending on outcome, may need to reimage.	EMAIL/PSA CALL

	Identify other suspicious events.			 ISOLATE
Inhibit System Recovery -vssadmin delete -wmic delete -wbadmin delete -bcdedit disable	Analyze image delete or disable Review timeline. Analyze details. Identify any other suspicious events.	Call IT Partner. If unauthorized/Partner not reachable, isolate device depending on hours of operations.	If not authorized, the device is compromised. Run a full AV scan. Change all user passwords with access to device. Investigate root cause and depending on outcome, may need to reimaging.	 EMAIL/PSA  CALL  ISOLATE
		Notify IT PARTNER if execution suspicious.	If authorized, please resolve incident. Apply incident suppression.	 EMAIL/PSA  CALL

IOC DETECTION, SUSPICIOUS TOOLS & NETWORK SERVICES				
DETECT	ANALYZE	REMEDATION / MITIGATION		ACTIONS
RocketCyber	RocketCyber	RocketCyber	IT PARTNER	RocketCyber
Suspicious Network Services	A suspicious network was detected.	Notify IT Partner.	Remove / uninstall if not authorized. Run a full AV scan on the system. Suppress if appropriate.	 EMAIL/PSA
Suspicious Tools	A suspicious tool was detected.	Notify IT Partner.	Remove / uninstall if not authorized. Run a full AV scan on the system. Suppress if appropriate.	 EMAIL/PSA

MALICIOUS FILE DETECTION				
DETECT	ANALYZE	REMEDATION / MITIGATION		ACTIONS
RocketCyber	RocketCyber	RocketCyber	IT PARTNER	RocketCyber
Malicious/ Suspicious File Detection	Analyze details. Review timeline. Identify any other suspicious events.	If file has a high malicious score and Partner is not answering the call to confirm authorized, Isolate device.	If unauthorized, remove the file, and run a full AV scan. If authorized, resolve incident, suppress incident notification.	 EMAIL/PSA  CALL  ISOLATE
		If file has a medium or low score, notify IT Partner.	If unauthorized, remove the file, and run a full AV scan. If authorized, resolve incident, suppress incident notification.	 EMAIL/PSA

OFFICE 365 LOGIN ANALYZER				
DETECT	ANALYZE	REMEDATION / MITIGATION		ACTIONS
RocketCyber	RocketCyber	RocketCyber	IT PARTNER	RocketCyber
Suspicious Successful O365 Login Detected	Analyze details (EMAIL/PSA & country). Review timeline.	Unauthorized login? EMAIL/PSA IT Partner. Call the first-time event is detected.	Kill Existing Sessions. Enable MFA for all users in the Tenant if not active. Add Conditional Access Policies to block by geolocation.	 EMAIL/PSA  CALL
		Expected Behavior? Notify IT Partner.	Suppress the EMAIL/PSA & country combination.	 EMAIL/PSA


Suspicious EMAIL/PSA Forwarding Rules Detected	Forwarding rules detected to EMAIL/PSA outside of corporate domain.	Notify IT Partner.	Review the rule. Remove if not authorized. Suppress if authorized.	 EMAIL/PSA
Risk Detection -unlikelyTravel -passwordSpray -leakedCredentials -impossibleTravel	Analyze details. Review timeline.	Notify IT Partner.	Review the alert on Azure AD. Reset user password if not authorized. Suppress if authorized.	 EMAIL/PSA

Remediation (RESPOND)

Device Isolation

- RocketCyber Managed SOC can isolate devices on a customer’s network that have a RocketCyber and/or Datto EDR Agent installed. The SOC uses host isolation to prevent the spread of malicious code by preventing a compromised machine from communicating to other network devices on the Internet or the Customer’s network.
- The isolated machine will maintain connectivity to the corresponding platform and allow the SOC or the Partner to reconnect the device. Unless the Partner opts-out in Special Instructions, the SOC will isolate potentially compromised devices.

File Deletion

- RocketCyber platform supports deleting some applications or files.
[RocketCyber Remediation Actions Overview](#)
- Datto EDR platform supports deleting files detected with the Datto EDR Reputation module.
 Alerts > Alert Detail > Respond  Respond > Delete File

Antivirus Actions

- RocketCyber or Datto EDR can run a Windows Defender AV quick or full scan if the integration is enabled.

Suppression

- RocketCyber Notification/Incident Suppression:
[Incident Suppression Overview](#)
- Datto EDR Suppressing alerts:
[Suppressing alerts](#)

Recommended Mitigations

CISA and FBI recommend that network defenders consider applying the following best practices to strengthen the security posture of their organization's systems whenever feasible:

- Provide social engineering and phishing training to employees.
- Consider drafting or updating a policy addressing suspicious EMAIL/PSAs that specifies users must report all suspicious EMAIL/PSAs to the security and/or IT departments.
- Mark external EMAIL/PSAs with a banner denoting the EMAIL/PSA is from an external source to assist users in detecting spoofed EMAIL/PSAs.
- Implement Group Policy Object and firewall rules.
- Implement an antivirus program and a formalized patch management process.
- Implement filters at the EMAIL/PSA gateway and block suspicious IP addresses at the firewall.
- Adhere to the principle of least privilege.
- Implement a Domain-Based Message Authentication, Reporting & Conformance validation system.
- Segment and segregate networks and functions.
- Limit unnecessary lateral communications between network hosts, segments, and devices.
- Consider using application allowlisting technology on all assets to ensure that only authorized software executes, and all unauthorized software is blocked from executing on assets. Ensure that such technology only allows authorized, digitally signed scripts to run on a system.
- Enforce multi-factor authentication.
- Enable a firewall on agency workstations configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Implement an Intrusion Detection System, if not already used, to detect C2 activity and other potentially malicious network activity
- Monitor web traffic. Restrict user access to suspicious or risky sites.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.
- Disable the use of SMBv1 across the network and require at least SMBv2 to harden systems against network propagation modules used by TrickBot.

Conclusion

We hope you enjoyed our Incident Response Guide. Reemphasizing our strategy to provide you with the best service with the most effective and efficient package to address your cybersecurity needs. We look forward to performing our part in protecting your networks and data. We thank you for your Partnership and for engaging us to provide a service to one of the most critical aspects of your business operations.

Please contact RocketCyber if you have any Platform issues or require assistance with an Active Security Incident. Support is available Mon-Fri 8:00 AM – 7:00 PM EST. The SOC is available 24x7 to monitor and respond to security incidents.

Create a ticket:

Support (Platform Issues, Integrations):

[Support \(Platform Issues, Integrations\)](#)

SOC (Active Security Events/Incidents):

[SOC \(Active Security Events/Incidents\):](#)

Or call us:

RocketCyber Support

US Toll-Free: (877) 282-8857 1, 7, 1, 2 - Mon-Fri 8:00 AM to 7:00 PM

RocketCyber Managed SOC (Active Security Incidents Assistance):

US Toll-Free: (877) 282-8857 1, 7, 1, 1

US Direct: +1 786 673 4043 (Outbound Caller ID)

EU Direct: +44 330 912 1898

AU Direct: +61 2 8000 9389