

Incident Response Guide

Version 1.0

Last Updated: 5 / 4 / 2022

Contents

Introduction	3
Partnership	3
Areas of Responsibility	4
Detections	5
Cyber Threat Intelligence	6
Event Data Collection, Analysis and Triage (DETECT)	7
Incident Response (RESPOND)	9
Automated Remediation (RESPOND).....	13
Recommended Mitigations	14
Conclusion	15

Threat Detection + REMEDIATION + Security Experts = Comprehensive Security Defense

Proactive & Preventative Security Management

- ✓ Improved Security Posture & Effectiveness of Security Tools/Strategies

24x7 x 365 SOC Coverage/Support

- ✓ (USA: Texas, Miami)

Overcome IT Skills & Resource Gaps

- ✓ Leverage Veteran IT & Cybersecurity Specialist and Analysts

Increased Threat Awareness & Risk Mitigation & REMEDIATION

- ✓ Real-time trending and expanded data analytics

Critical Documentation & Record keeping for:

- ✓ Event Log & Activity Tracking and
- ✓ Incident / Notification Records

Introduction

RocketCyber SOC team works alongside Complete IT's support group 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 dual automated and manual approach provide 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 Complete IT 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 Complete IT to ensure the most effective ability to **DETECT**, **RESPOND**, and **RECOVER** to a cyber event.

FUNCTION	RESPONSIBLE ENTITY	CATEGORY
IDENTIFY	COMPLETE IT	Asset Management
	COMPLETE IT	Business Environment
	COMPLETE IT	Governance
	COMPLETE IT	Risk Assessment
	COMPLETE IT	Risk Management Strategy
	COMPLETE IT	Supply Chain Risk Management
PROTECT	COMPLETE IT	Identity Management, Authentication & Access Control
	COMPLETE IT	Awareness and Training
	COMPLETE IT	Data Security
	COMPLETE IT	Information Protection Processes and Procedures
	COMPLETE IT	Maintenance
	COMPLETE IT	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/Remediation
	COMPLETE IT	Mitigation/Remediation
	RocketCyber SOC	Improvements
	COMPLETE IT	Improvements
RECOVER	COMPLETE IT	Recovery Planning
	COMPLETE IT	Improvements
	COMPLETE IT	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 attachments or links resulting in some form of malware or establishes 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** - involve 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 Compromise (BEC)** – an attacker has gained unauthorized access to an employee’s email.
- **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 Tunneling** – 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 or 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, the malware is served in content such as banners and advertisements. These days exploit kits are available which allow novice hackers to easily setup 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 the 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.
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.
MALICIOUS FILE DETECTION	The RocketCyber Agent monitors and detects suspicious and malicious files that are written to disk or executed.
MICROSOFT EXCHANGE HAFNIUM EXPLOIT DETECTION	The RocketCyber Agent will look for specific Indicators of compromise (IOCs) related to exploitation of Microsoft Exchange 2010, 2013, 2016 and 2019 via CVE CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. It will also report the patch status for mitigations against these vulnerabilities.
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.
BITDEFENDER MONITOR	The SOC Platform ingests and reports on detections from BitDefender.







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 COMPLETE IT. 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 manager will authorize taking the device offline to stop the spreading of the threat even in the event when no one can be reached, unless otherwise specified by the Complete IT. The SOC will continue to call the available numbers until a team member of our Complete IT is reached. We consider every Incident that requires a phone call from the SOC to Complete IT Severity 1 case.

Upon generation of an event that is classified as an incident, the RSOC team will begin investigation within minutes of detection and will provide update within the given timeframe. This is measured by taking the difference between creation of the incident as shown in the audit log and when the incident is either assigned to a RSOC analyst or manually escalated.

SEVERITY LEVELS – INCIDENTS				
Severity	Impact	Description	Typical Response (Detection/ Notification/ Action)	Contractual SLA
SEV 1	Critical-Urgent	System was breached, attack in progress. (Ransomware, Squiblydoo attack, etc.)	1 Min / 5 Min / 10 Min	60 Minutes
SEV 1	Critical	AV quarantine action failed, O365 forwarding rules detected, O365 Successful login from other countries detected.	1 Min/ 5 Min / 10 Min	60 Minutes
SEV 2	Major	Unusual activity, but no breach by malicious party was detected, and no system components were compromised.	2 Min / 10 Min / As Needed	Not Applicable
SEV 3	Minor	System is showing failed logon attempts or other events generated by customer network systems or users and not part of a cybersecurity threat.	2 Min / 10 Min / As Needed	Not Applicable
SEV 4	Informational	No effect on the system is recorded – informational data only which may be useful for investigation.	5 Min / As Needed/ As Needed	Not Applicable

ADVANCED BREACH DETECTION				
DETECT	ANALYZE	REMEDIACTION / MITIGATION		NOTIFICATION
RocketCyber	RocketCyber	RocketCyber	COMPLETE IT	RocketCyber
SUSPICIOUSLY SIGNED BINARY PROXY EXECUTION	Analyze file execution. Review timeline of file execution.	If execution malicious, notify COMPLETE IT. Disconnect device from network.	Review the file and remove if not needed. Run a full AV scan. Change any admin passwords with access to machine.	 EMAIL  CALL
		If execution suspicious, notify COMPLETE IT.	Review event and whitelist if execution is authorized	 EMAIL
INHIBIT SYSTEM RECOVERY DETECTED	Analyze executions of vssadmin.exe, wbadmin.exe, or bcdedit.exe	If executions are preceded and/or followed by other suspicious actions, notify COMPLETE IT. Disconnect device from network.	Review the detection. If not authorized, run a full AV scan of the system and other clean-up tools available. Change any admin passwords with access to machine.	 EMAIL  CALL
		If executions are only suspicious, notify COMPLETE IT.	Review the detection. If not authorized, run a full AV scan of the system and other clean-up tools available.	 EMAIL



MALICIOUS FILE DETECTION				
DETECT	ANALYZE	REMEDIACTION / MITIGATION		NOTIFICATION
RocketCyber	RocketCyber	RocketCyber	COMPLETE IT	RocketCyber
MALICIOUS FILE DETECTION	Investigate if single file or multiple file execution(s).	If confirmed malware: Notify COMPLETE IT. Disconnect device from network.	Remove entries from Registry. Run AV scan, Malwarebytes Free/Premium, Microsoft MSRT. Remove remaining malicious files manually.	 EMAIL  CALL
		If suspicious execution but not confirmed as malware: No SOC remediation. Notify COMPLETE IT.	If confirmed malware: Remove entries from Registry. Run AV scan & Malwarebytes Free/Premium. Remove remaining malicious files.	 EMAIL
SUSPICIOUS FILE DETECTION	Test file using threat intelligence.	The file XXXXX.exe was flagged as suspicious on device XXXXX. Investigate if single file or multiple file execution(s).	Please review and verify the file. Remove if not required. Run a full AV scan on the system. Make sure the system is fully patched. Whitelist if appropriate	 EMAIL  CALL




CYBER TERRORIST NETWORK CONNECTIONS				
DETECT	ANALYZE	REMEDIACTION / MITIGATION		NOTIFICATION
RocketCyber	RocketCyber	RocketCyber	COMPLETE IT	RocketCyber
SUCCESSFUL MALICIOUS RDP SESSION	Test Remote IP using threat intelligence. If logon attempted from country in high-risk category	No successful login detected: Notify COMPLETE IT.	Place RDP behind VPN. Make sure system is fully patched. Implement strict firewall policies to reduce the attack surface. Consider implementing geo-based policies if applicable.	 EMAIL
		If successful login detected: Notify COMPLETE IT.	Place RDP behind VPN. Fully patch system. Implement strict firewall policies to reduce the attack surface. Consider implementing geo-based policies if applicable.	 EMAIL  CALL

INBOUND CONNECTIONS FROM xx ON 445 or 25	Inbound connections were detected on port 445 or 25.	If successful logins detected: Notify COMPLETE IT. Identify if any other executions took place.	Block port 445 at the firewall. Implement strict firewall policies to reduce the attack surface by limiting both inbound and outbound traffic to only necessary ports and protocols.	EMAIL CALL
		If failed logins detected: Notify COMPLETE IT	Block port 445 at the firewall. Implement strict firewall policies to reduce the attack surface by limiting both inbound and outbound traffic to only necessary ports and protocols. Remove any files or registry entries Remove any entries from Registry. Run AV scan, Malwarebytes Free/Premium, Microsoft MSRT. Remove remaining malicious files manually.	EMAIL

AV MONITOR				
DETECT	ANALYZE	REMEDATION / MITIGATION		NOTIFICATION
RocketCyber	RocketCyber	RocketCyber	COMPLETE IT	RocketCyber
MONITOR: - SENTINELONE - BITDEFENDER - CYLANCE - SOPHONS - WEBROOT - DEEP INSTINCT	If threat is identified as Ransomware, mitigated or not, call customer and Isolate Device.	Investigate any other potentially malicious events on any other devices.	Review the detection. Run a full AV scan of the system and anti-malware utility. Delete registry keys and programs that may have been installed. Whitelist if appropriate.	CALL ISOLATE EMAIL
	Determine if threat was mitigated – if not, notify COMPLETE IT.	Investigate any other potentially malicious events.	Review the detection. Run a full AV scan of the system and anti-malware utility. Delete registry keys and programs that may have been installed. Whitelist if appropriate.	EMAIL CALL
	Determine if threat was mitigated – if yes, notify IT PARTNER.	No action.	Review the detection. Run a full AV scan of the system. Whitelist if appropriate.	EMAIL

OFFICE 365 LOGIN ANALYZER				
DETECT	ANALYZE & COMMUNICATE	REMEDATION / MITIGATION		NOTIFICATION
RocketCyber	RocketCyber	RocketCyber	COMPLETE IT	RocketCyber
SUSPICIOUS SUCCESSFUL OFFICE 365 LOGIN DETECTED	The following account successfully logged in from country X. Detected logins outside the expected countries or from known malicious IP addresses.	Notify COMPLETE IT.	Whitelist the alerts for user from detected location. From Incident View, click on Action/Whitelist to whitelist.	Email
EMAIL FORWARDING RULE DETECTED	Forwarding rule detected to email outside of corporate domain.	Notify COMPLETE IT.	Review the rule. Remove if not authorized. Whitelist if authorized.	Email CALL

O365 LICENSE	The current Office 365 configuration does not allow monitoring of Office 365 Logins for this customer.	Without the proper licensing, the SOC will not be able to monitor for suspicious login activity. Notify COMPLETE IT.	The Tenant requires at least one Azure P1 or P2 license to access login data. Follow instructions provided to add the required license.	 Email
OFFICE 365 BRUTE FORCE ATTEMPT	Multiple failed logon attempts from various countries; the account is locked.	Notify COMPLETE IT.	Enable 2 Factor Authentication for all users in the Tenant. Add Conditional Access Policies to block by undesired logon regions. Kill Existing Sessions.	 Email

SUSPICIOUS TOOLS				
DETECT	ANALYZE	REMEDIAION / MITIGATION		NOTIFICATION
RocketCyber	RocketCyber	RocketCyber	COMPLETE IT	RocketCyber
SOCIAL ENGINEERING TOOLS DETECTED	A suspicious tool classified as Social Engineering Tools was detected.	Review the history for the device. Notify COMPLETE IT.	Review the tool detection. Remove / uninstall if not authorized. Run a full AV scan on the system. Whitelist if appropriate	 Email
SUSPICIOUS TOOL: BITCOIN MINING	Investigate if the bitcoin-mining tool is suspicious or authorized.	Review the history for the device. Notify COMPLETE IT.	Review the tool detection. Remove / uninstall if not authorized. Run a full AV scan on the system. Whitelist if appropriate.	 Email
SUSPICIOUS TOOL(S) DETECTED: NMAP, WIRESHARK	Investigate if the utility tool detected is suspicious or authorized.	Review the history for the device. Notify COMPLETE IT.	Review the tool detection. Remove / uninstall if not authorized. Run a full AV scan on the system. Whitelist if appropriate	 Email

Automated Remediation (RESPOND)

Device Isolation - RocketCyber RSOC can isolate machines on a customer's network that have a RocketCyber Agent installed. The RSOC 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 RSOC and allow our analysts to continue investigation without risking other network devices to malicious code or active attacks. Unless the Customer opts-out, RocketCyber will isolate potentially compromised machines. RocketCyber will manually isolate the machine using the installed RocketAgent and notify the customer of the isolation via an incident for escalation. The machines will remain in isolation until the threat has been remediated or the customer has specifically said they accept the risk and request the RSOC to remove the isolation.

Automated Remediation - For certain incidents, the RocketAgent can perform automated remediation tasks. These remediation actions are visible in the Incident view by clicking the Remediate Action. Customers can opt-in to allow the SOC Analysts to execute the automated remediation actions on affected endpoints. The current remediation actions that can be performed are:

- Terminate Processes
- Remove Files
- Uninstall Programs
- Modify Registry Keys
- Stop Services
- Remove Scheduled Tasks

Antivirus Actions - Some AV Product integrations with the RCC allow RSOC Analysts to perform AV related actions such as Quarantine, Kill, Remediate and Whitelist. The following guidelines apply to integrations that support those features.

- Active Threats (Those not killed, quarantined, or remediated) automatically by the AV agent will be reviewed. Hashes will be verified using various threat intel sources. If found to be benign the RSOC analyst will whitelist. If found to be malicious or unknown the RSOC team will quarantine. If AV Product supports classifications by an RSOC Analysts, the file will be classified as determined by the analyst. An incident will be generated indicating the status of the threat and the action taken by the RSOC analyst.
- Suspicious Threats (Those reported, but not killed, quarantined, or remediated) automatically by the AV agent will be reviewed. Hashes will be verified using various threat intel sources. If found to be benign the SOC team will whitelist. If found to be malicious or unknown the RSOC team will quarantine. If AV Product supports classifications by an RSOC Analysts, the file will be classified as determined by the analyst. An incident will be generated indicating the status of the threat and the action taken by the RSOC analyst.
- All other threats (killed, quarantined, or remediated) automatically by the AV agent will be reported as an incident for customer review and notification.
- Temp files that are detected but not (killed, quarantined, or remediated) automatically by the AV agent will be investigated using best efforts and threat intelligence sources. Incidents will only be generated if the file can be positively identified by the RSOC analyst.
- Other non-file-based threat detections by AV products such as Lateral Movement. An incident will be generated indicating the status of the threat.

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 emails that specifies users must report all suspicious emails to the security and/or IT departments.
- Mark external emails with a banner denoting the email is from an external source to assist users in detecting spoofed emails.
- Implement Group Policy Object and firewall rules.
- Implement an antivirus program and a formalized patch management process.
- Implement filters at the email 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 hoses, segments, and devices.
- Consider using application allow listing 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 possible, RocketCyber's SOAR solution enables the SOC to provide a proactive constantly adapting solution to a cybersecurity landscape that is much too often reactive to the ever-evolving threats. The SOC combines cutting-edge artificial intelligence, machine learning, and the unique experience of our cybersecurity-certified analysts to provide you 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 the SOC if you have any questions about incidents that were created or security related events you have discovered. The SOC is available 24x7 to answer your questions. You can reach the SOC via phone call, email, the Web ([Open Ticket](#)), RocketCyber Dashboard ([Help](#)):

Complete IT

Web: <https://completeit.com/>

Email: service@completeit.com

Phone: 512-674-4134

RocketCyber Managed SOC

Web: <https://support.rocketcyber.com/>

Email: support@rocketcyber.com

US: +1 214 295 5333

US: +1 877 282 8857 (Toll-Free)

UK: + 44 (20) 4540 0707