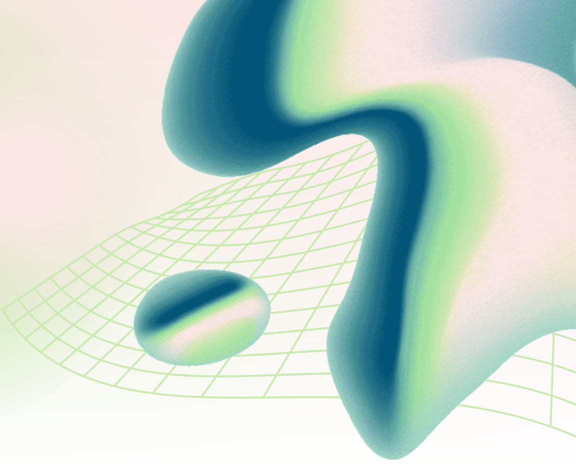
DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR) REPORT



Conducted by Anthony Whiteman

Summary

As part of my professional portfolio, I conducted a simulated security incident investigation for the game studio Giggly Goofo. The scenario involved the exfiltration of confidential files by both internal and external actors. Provided with a PCAP file of network traffic and a drive image from a simulated employee, I leveraged NetWitness Investigator to perform a comprehensive forensic analysis. The investigation focused on identifying malicious activity, mapping attack vectors, and contextualizing threat behavior. This exercise provided hands on experience with enterprise level forensic tools and incident response methodologies.

Note: The findings in this report are based on simulated data and should not be interpreted as factual events.

Objective & Methodology

The primary objective of this Digital Forensics and Incident Response (DFIR) investigation was to analyze a simulated data breach at the game development studio, Giggly Goofo. The goal was to determine the scope of the compromise, identify the methods of data exfiltration, and confirm the involvement of a suspected internal employee. The investigation followed this structured methodology:

1. **Evidence Review:** The investigation began with two key pieces of evidence: a network traffic capture (IRcapture.pcap) and a forensic disk image (MJ_evidence.001) from the workstation of the suspected employee, Marvin Jonson.

2. **Network Analysis:** The PCAP file was analyzed using NetWitness Investigator to reconstruct the network sessions, identify external IP addresses, and uncover the specific method of data exfiltration.

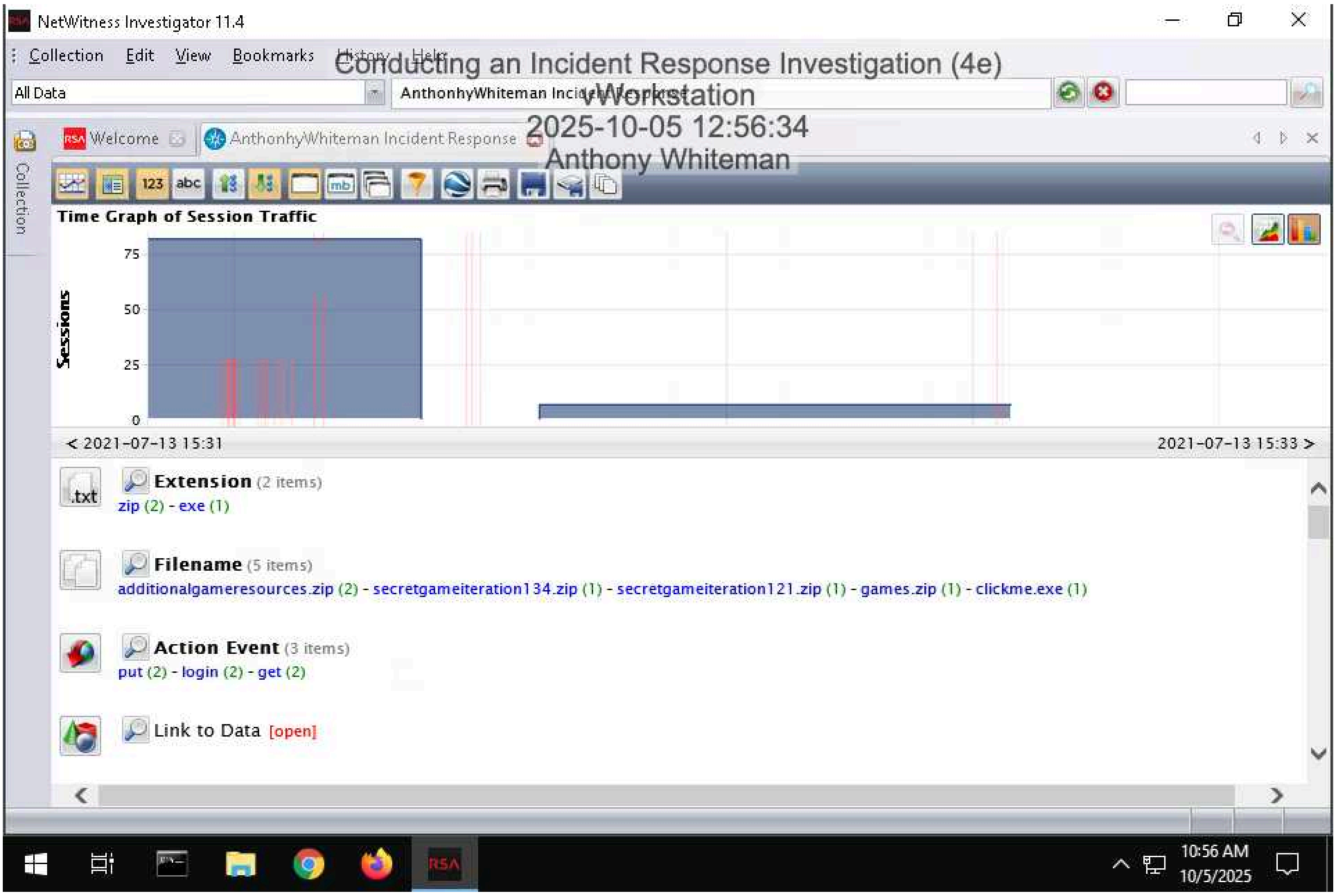
3. **Disk Forensics:** The employee's disk image was analyzed using Paraben's E3 to search for evidence of collusion, focusing on email databases and system files to correlate findings from the network analysis.

4. **Reporting:** The findings were documented in a comprehensive report, including a summary of the incident, the methodology used, and recommendations for preventing similar incidents in the future.

Investigation Findings

The investigation revealed the following key findings:

Point of Compromise: Valid Accounts (T1078) & Exfiltration Over Alternative Protocol (T1048)
My analysis of the provided PCAP file shows the external actor gained initial access to Giggly Goofo's network using legitimate FTP credentials (GigglyGoofoDev / Il0veC0d!nG). My examination of the disk image confirmed these credentials were provided by employee Marvin Jonson, who sent them to the actor via email. Using this access, the actor connected from IP address 157.165.0.25 and exfiltrated multiple sensitive files, including: (secretgameiteration121.zip and secretgameiteration134.zip), over the unencrypted FTP protocol.



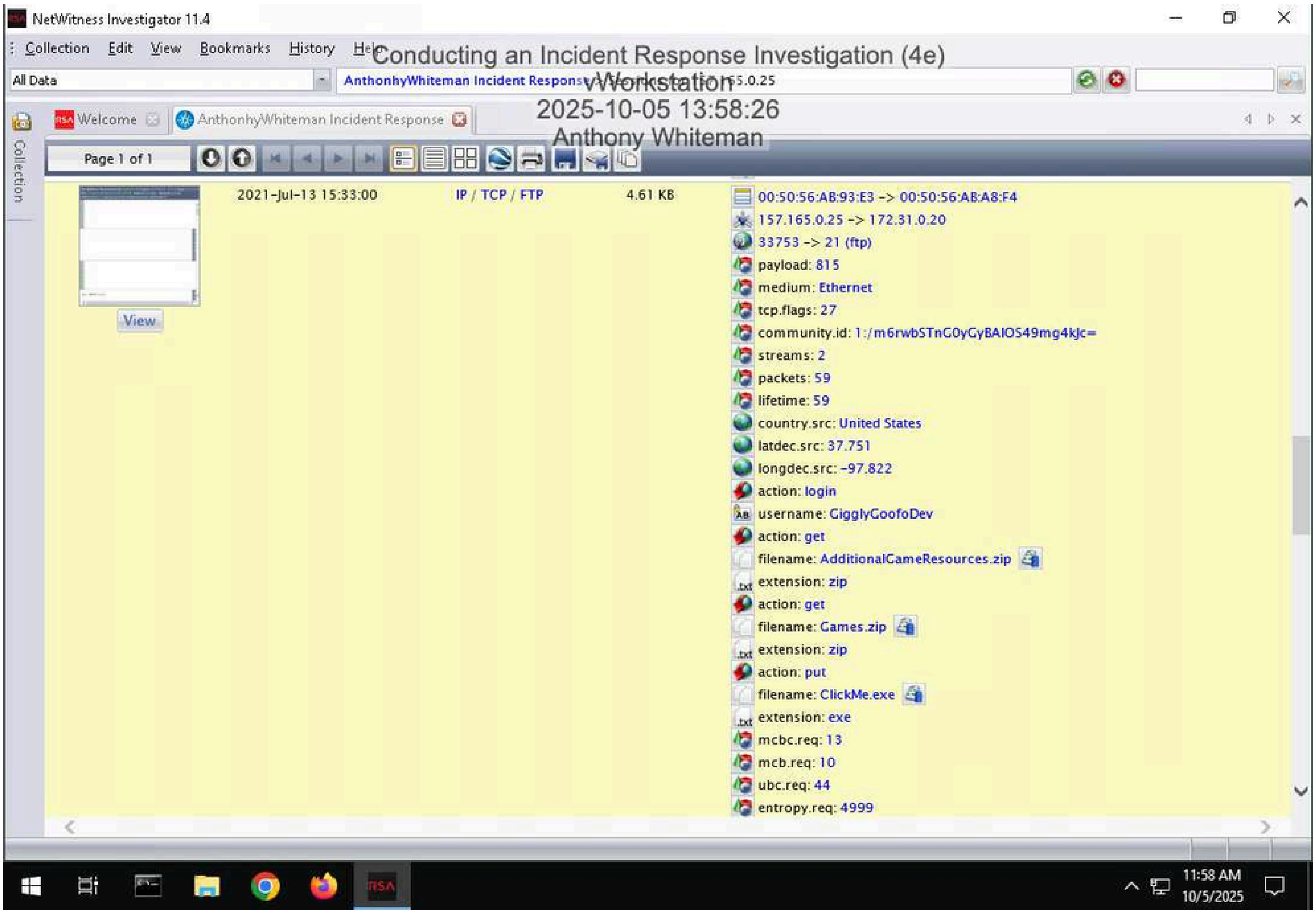
Extension (2 items)
zip (2) - exe (1)

Filename (5 items)
additionalgameresources.zip (2) - secretgameiteration134.zip (1) - secretgameiteration121.zip (1) - games.zip (1) - clickme.exe (1)

Action Event (3 items)
put (2) - login (2) - get (2)

Link to Data [open]

- ***Figure 1: Time Graph in NetWitness Investigator displaying network traffic sessions from July 13, 2021, and identifying transferred files.***



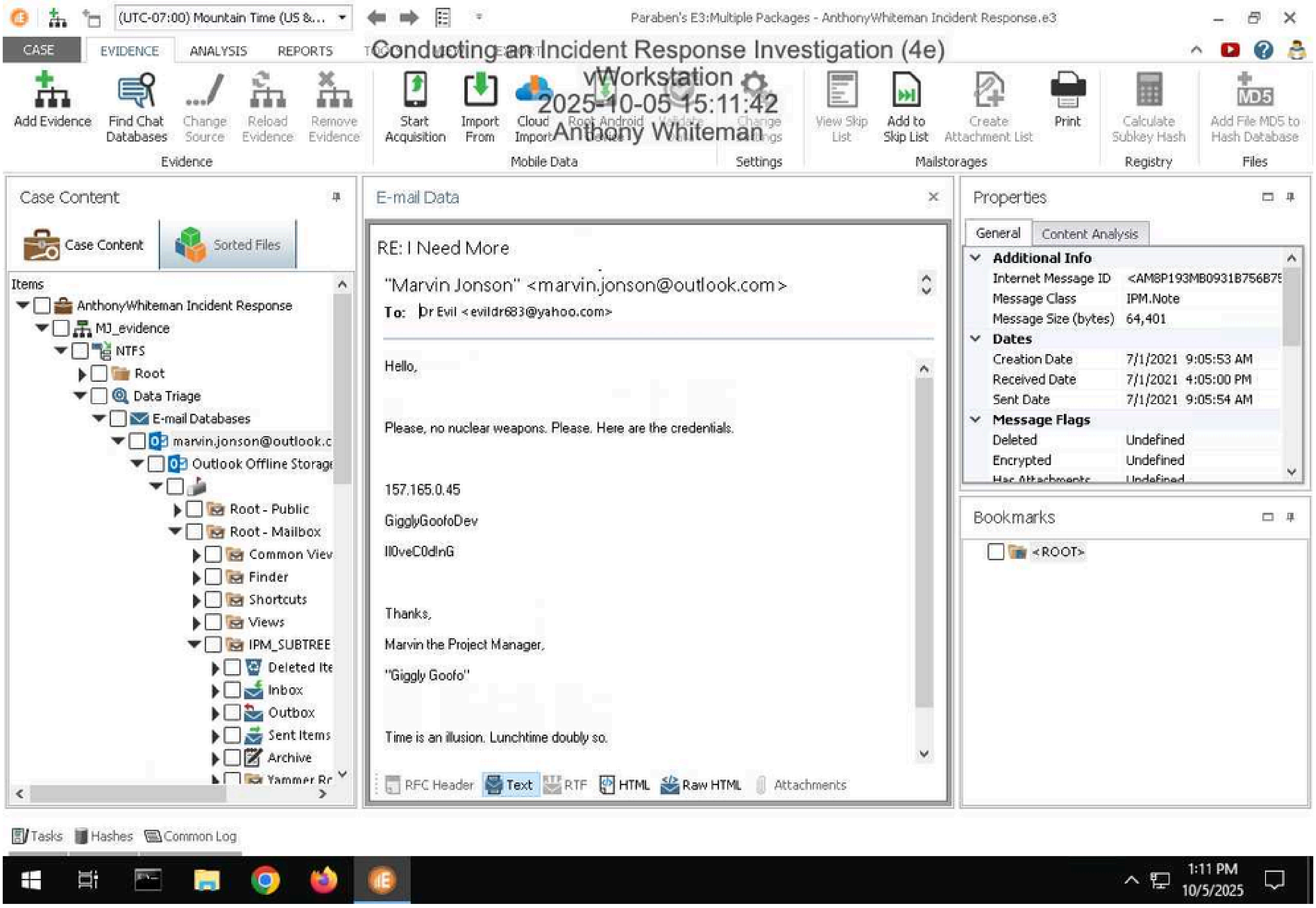
Conducting an Incident Response Investigation (4e)
Workstation
2025-10-05 13:58:26
Anthony Whiteman

AnthonhyWhiteman Incident Response / Sessions for 157.165.0.25

2021-Jul-13 15:33:00 IP / TCP / FTP 4.61 KB

00:50:56:AB:93:E3 -> 00:50:56:AB:A8:F4
157.165.0.25 -> 172.31.0.20
33753 -> 21 (ftp)
payload: 815
medium: Ethernet
tcp.flags: 27
community.id: 1:/m6rwbSTnG0yGyBAIOS49mg4kJc=
streams: 2
packets: 59
lifetime: 59
country.src: United States
latdec.src: 37.751
longdec.src: -97.822
action: login
username: GigglyGoofoDev
action: get
filename: AdditionalGameResources.zip
extension: zip
action: get
filename: Games.zip
extension: zip
action: put
filename: ClickMe.exe
extension: exe
mcbc.req: 13
mcb.req: 10
ubc.req: 44
entropy.req: 4999

- ***Figure 2: Detailed analysis of the FTP session from 15:33:00, showing the external actor's IP (157.165.0.25), the compromised username (GigglyGoofoDev), and the names of the exfiltrated files.***



RE: I Need More

"Marvin Jonson" <marvin.jonson@outlook.com>
To: Dr Evil <evildr683@yahoo.com>

Hello,

Please, no nuclear weapons. Please. Here are the credentials.

157.165.0.45

GigglyGoofoDev

Il0veC0dInG

Thanks,

Marvin the Project Manager,

"Giggly Goofo"

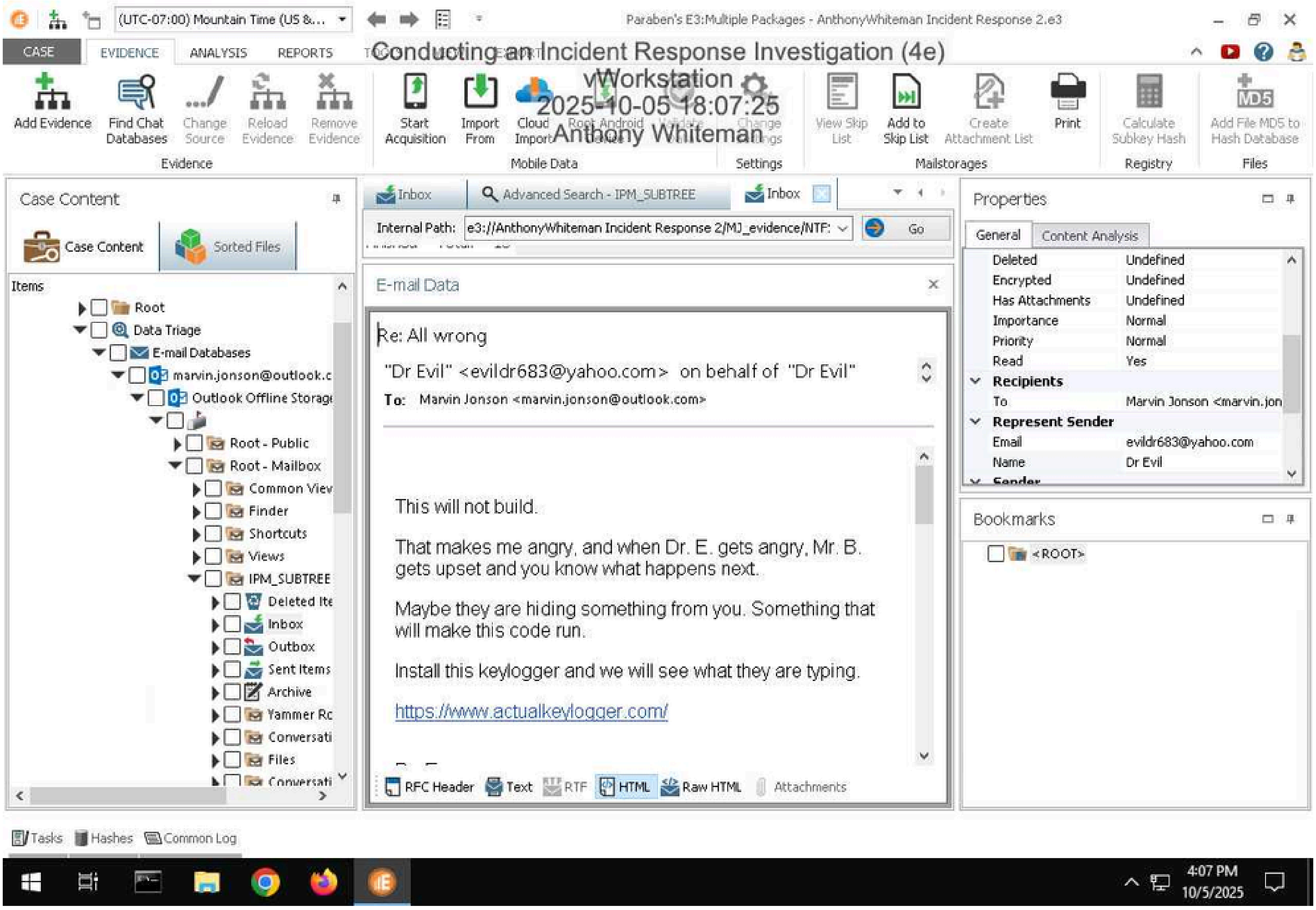
Time is an illusion. Lunchtime doubly so.

Additional Info	
Internet Message ID	<AM8P193MB0931B756B75
Message Class	IPM.Note
Message Size (bytes)	64,401
Dates	
Creation Date	7/1/2021 9:05:53 AM
Received Date	7/1/2021 4:05:00 PM
Sent Date	7/1/2021 9:05:54 AM
Message Flags	
Deleted	Undefined
Encrypted	Undefined
Has Attachments	Undefined

- ***Figure 3: Email recovered from Marvin Jonson's disk image showing the explicit sharing of FTP credentials with the external actor "Dr. Evil."***

Execution & Persistence: User Execution (T1204) & Scheduled Task (T1053.005)

Following the data exfiltration, the external actor instructed Marvin Jonson via email to execute a malicious payload on his corporate workstation. To establish persistence, Jonson created a Scheduled Task, configuring his system to automatically run the payload. Analysis of the task's properties confirmed Jonson as the author.



Internal Path: e3://AnthonyWhiteman Incident Response 2/MJ_evidence/NTF:

Re: All wrong

"Dr Evil" <evildr683@yahoo.com> on behalf of "Dr Evil"

To: Marvin Jonson <marvin.jonson@outlook.com>

This will not build.

That makes me angry, and when Dr. E. gets angry, Mr. B. gets upset and you know what happens next.

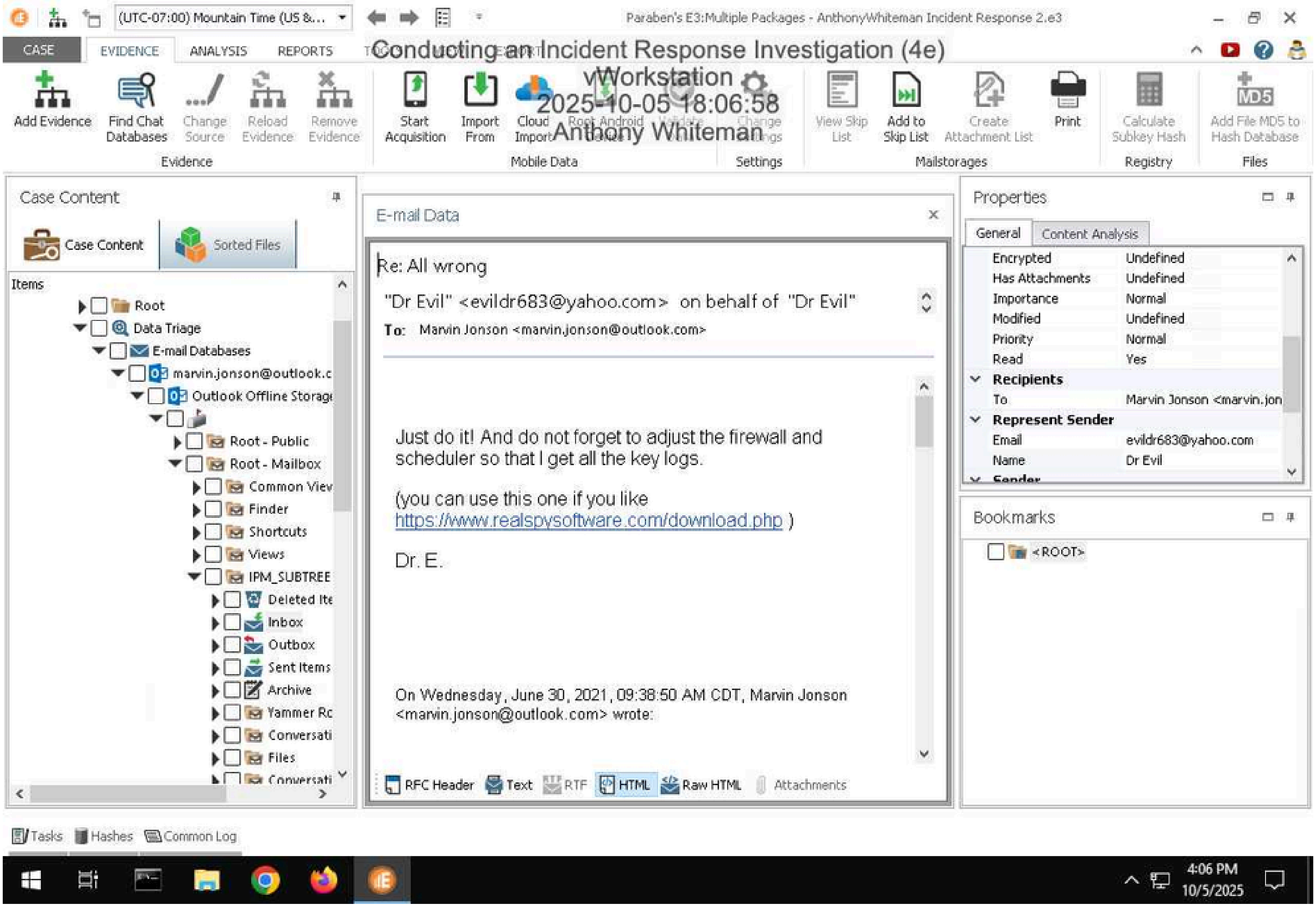
Maybe they are hiding something from you. Something that will make this code run.

Install this keylogger and we will see what they are typing.

https://www.actualkeylogger.com/

Deleted	Undefined
Encrypted	Undefined
Has Attachments	Undefined
Importance	Normal
Priority	Normal
Read	Yes
Recipients	
To	Marvin Jonson <marvin.jon
Represent Sender	
Email	evildr683@yahoo.com
Name	Dr Evil
Sender	

- ***Figure 4: Email from "Dr. Evil" instructing Marvin Jonson to install a keylogger from www.actualkeylogger.com.***



Re: All wrong

"Dr Evil" <evildr683@yahoo.com> on behalf of "Dr Evil"

To: Marvin Jonson <marvin.jonson@outlook.com>

Just do it! And do not forget to adjust the firewall and scheduler so that I get all the key logs.

(you can use this one if you like https://www.realspysoftware.com/download.php)

Dr. E.

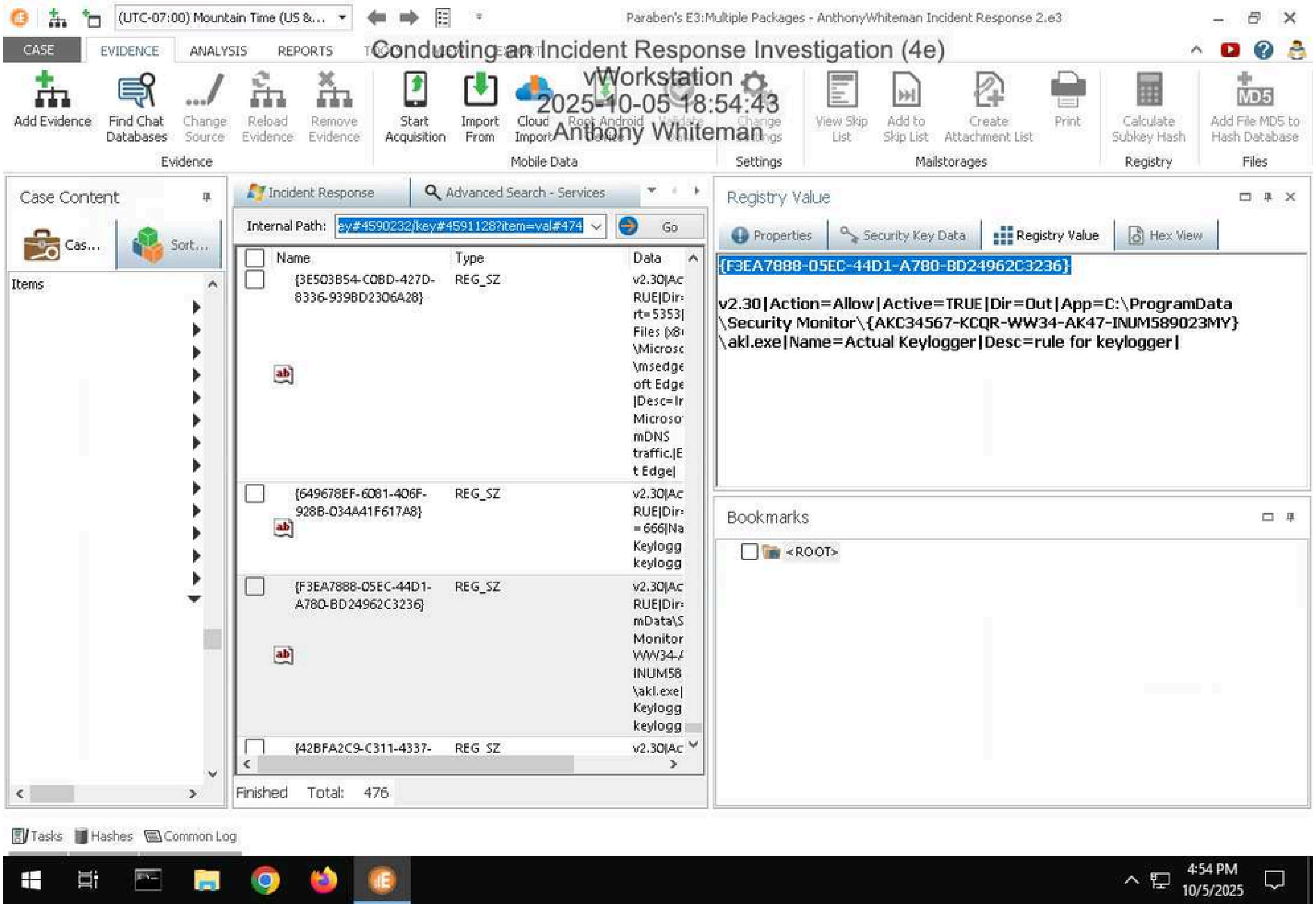
On Wednesday, June 30, 2021, 09:38:50 AM CDT, Marvin Jonson <marvin.jonson@outlook.com> wrote:

Encrypted	Undefined
Has Attachments	Undefined
Importance	Normal
Modified	Undefined
Priority	Normal
Read	Yes
Recipients	
To	Marvin Jonson <marvin.jon
Represent Sender	
Email	evildr683@yahoo.com
Name	Dr Evil
Sender	

- ***Figure 5: Follow-up email from "Dr. Evil" directing Jonson to "adjust the firewall and scheduler" to ensure the keylogger's functionality.***

Collection & Defense Evasion: Keylogging (T1056.001) & Modify System Firewall (T1562.004)

The deployed payload was identified as a keylogger, a form of spyware designed to capture user keystrokes. To evade security controls and enable command-and-control, Jonson created a new rule in the Windows firewall to allow inbound connections for the keylogger executable. Windows 10 Activity Timeline analysis confirmed Jonson repeatedly interacted with the keylogger application, indicating active use beyond the initial installation.



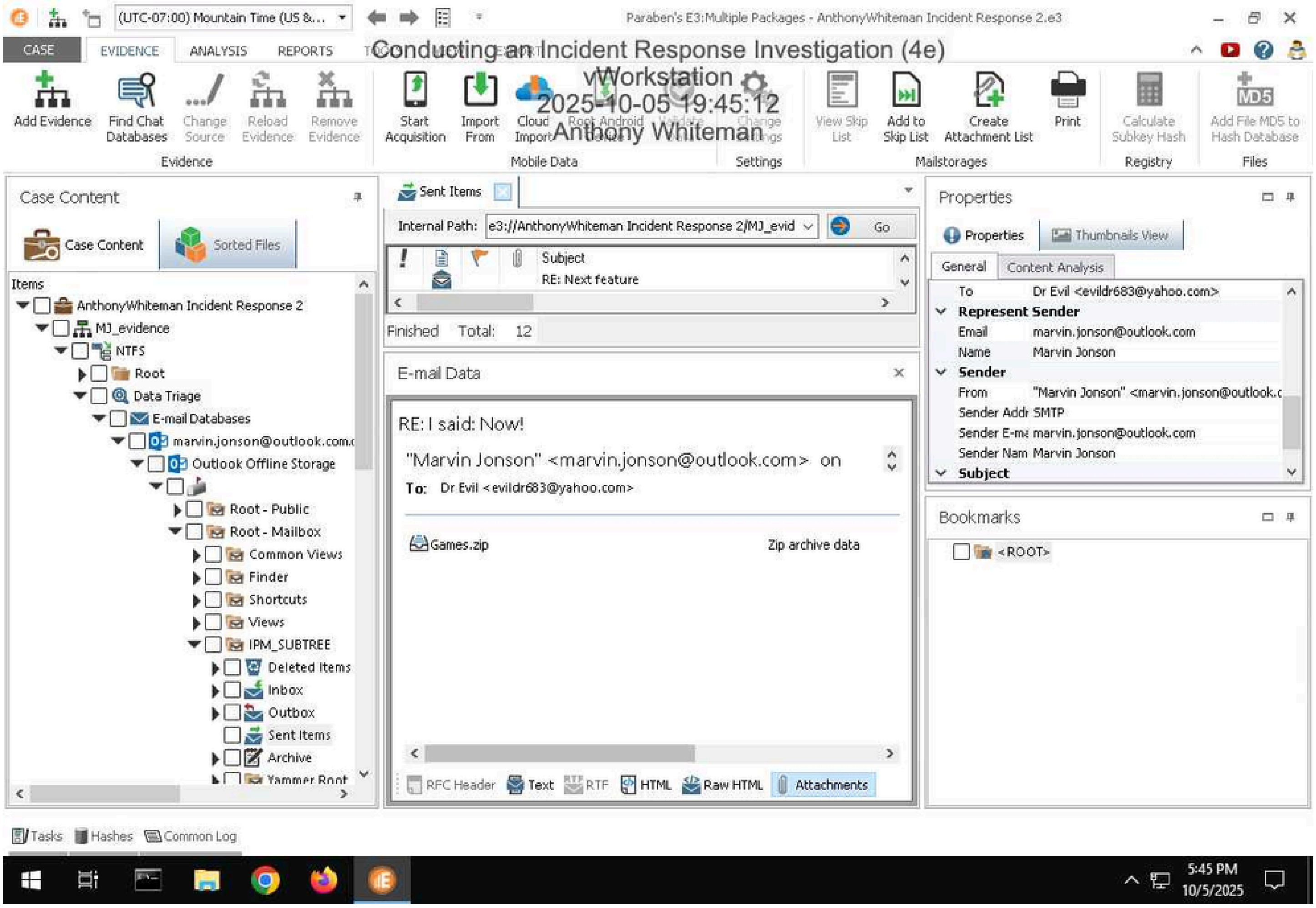
	Name	Type	Data
□	{3E503B54-C0BD-427D-8336-939BD2306A28}	REG_SZ	v2.30|Ac RUE|Dir= rt=5353| Files (x8 \Microsc \msedge oft Edge |Desc=Ir Microso mDNS traffic.|E t Edge|
□	{649678EF-6081-406F-928B-034A41F617A8}	REG_SZ	v2.30|Ac RUE|Dir= =666|Na Keylogg keylogg
□	{F3EA7888-05EC-44D1-A780-BD24962C3236}	REG_SZ	v2.30|Ac RUE|Dir= mData\S Monitor WW34-A INUM58 \akl.exe| Keylogg keylogg
□	{42BFA2C9-C311-4337-	REG_SZ	v2.30|Ac

Finished Total: 476

```
{F3EA7888-05EC-44D1-A780-BD24962C3236}

v2.30|Action=Allow|Active=TRUE|Dir=Out|App=C:\ProgramData
\Security Monitor\{AKC34567-KCQR-WW34-AK47-INUM589023MY}
\akl.exe|Name=Actual Keylogger|Desc=rule for keylogger|
```

- ***Figure 6: Windows Registry key displaying the firewall rule created to allow network traffic for the "Actual Keylogger" application.***



Internal Path: e3://AnthonyWhiteman Incident Response 2/MJ_evid

Subject: RE: Next feature

Finished Total: 12

RE: I said: Now!

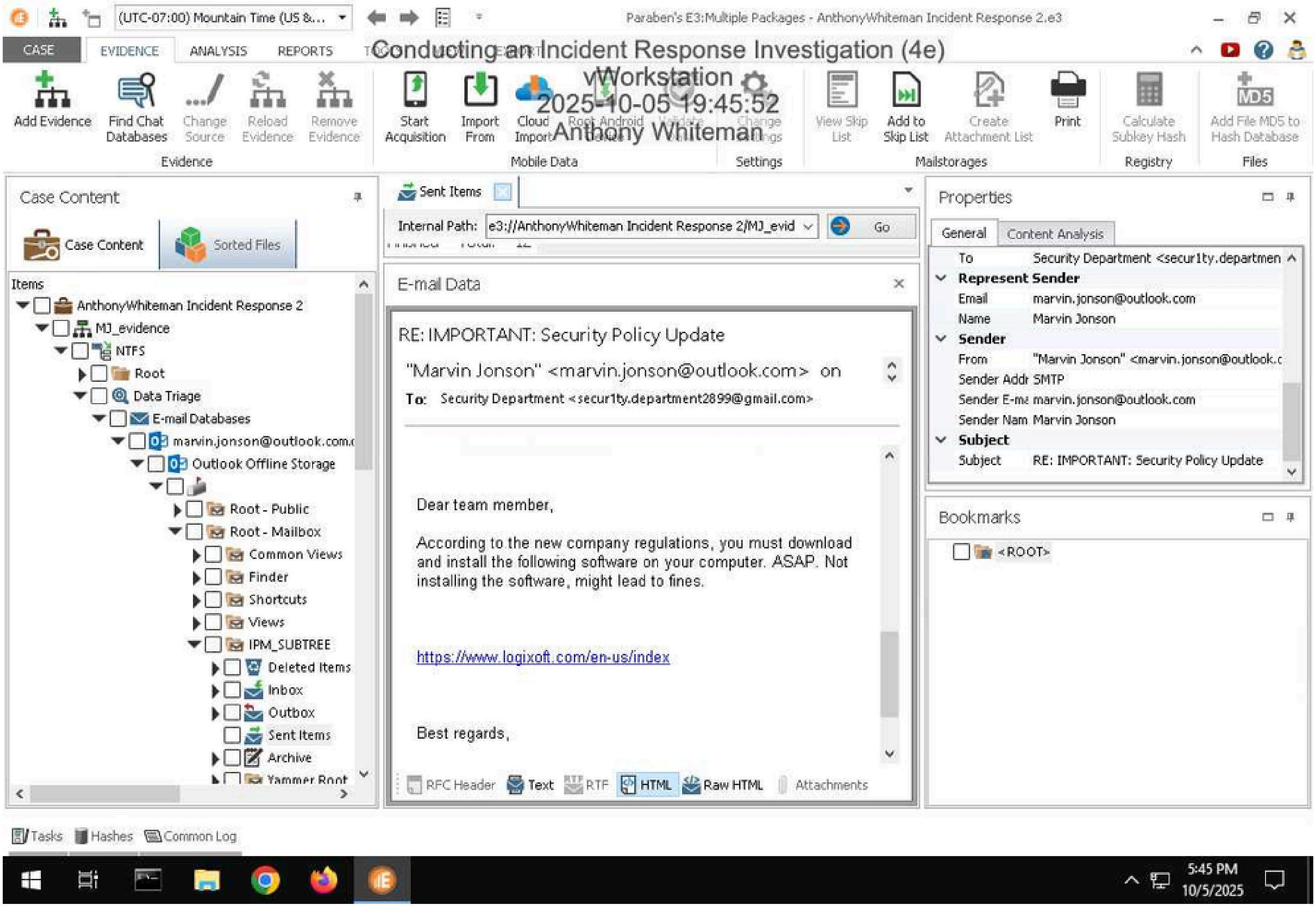
"Marvin Jonson" <marvin.jonson@outlook.com> on

To: Dr Evil <evildr683@yahoo.com>

Games.zip Zip archive data

To	Dr Evil <evildr683@yahoo.com>
Represent Sender	
Email	marvin.jonson@outlook.com
Name	Marvin Jonson
Sender	
From	"Marvin Jonson" <marvin.jonson@outlook.c
Sender Addr	SMTP
Sender E-ma	marvin.jonson@outlook.com
Sender Nam	Marvin Jonson
Subject	

- **Figure 7: Evidence of data exfiltration via email, showing Marvin Jonson sending the file Games.zip as an attachment to "Dr. Evil."**



RE: IMPORTANT: Security Policy Update

"Marvin Jonson" <marvin.jonson@outlook.com> on

To: Security Department <secur1ty.department2899@gmail.com>

Dear team member,

According to the new company regulations, you must download and install the following software on your computer. ASAP. Not installing the software, might lead to fines.

https://www.logixoft.com/en-us/index

Best regards,

To	Security Department <secur1ty.departmen
Represent Sender	
Email	marvin.jonson@outlook.com
Name	Marvin Jonson
Sender	
From	"Marvin Jonson" <marvin.jonson@outlook.c
Sender Addr	SMTP
Sender E-ma	marvin.jonson@outlook.com
Sender Nam	Marvin Jonson
Subject	
Subject	RE: IMPORTANT: Security Policy Update

- ***Figure 8: Phishing email disguised as a "Security Policy Update," instructing the installation of additional suspicious software.***

Recommended Remediations

My investigation concluded that the root cause of this incident was not a technical exploit, but a targeted social engineering attack against a Project Manager, Marvin Jonson. This attack successfully cultivated a malicious insider who then facilitated the data breach and malware installation. To address these specific risks, I recommend a defense strategy focused on strengthening human defenses, implementing a Zero Trust security policy, and enhancing technical threat detection.

Strengthen Human Defenses:
Since this attack exploited human trust, the first line of defense is to build employee resilience against manipulation.

- **Security Awareness Training:** I recommend implementing a continuous security awareness program. This training must focus on helping employees recognize social engineering tactics, such as the coercive language used by "Dr. Evil" in the recovered emails, and understand the procedures for reporting suspicious contact.

- **Phishing Simulations:** This training should be reinforced with regular, realistic phishing simulations to test and improve employee response to threats like the fraudulent "Security Policy Update" email.

Adopt a Zero Trust Policy to Limit Compromise Impact:
A Zero Trust security policy operates on the principle of "never trust, always verify," which would have significantly limited the damage from this incident.

- **Enforce Multi-Factor Authentication (MFA):** Mandate MFA on all critical systems, especially externally-facing services like the FTP server. This is the single most effective technical control that would have prevented the external actor from using the compromised GigglyGoofoDev password.

- **Decommission Shared Accounts:** Shared accounts like GigglyGoofoDev should be eliminated. All access must be tied to individual, named users to ensure accountability.

- **Apply the Principle of Least Privilege:** Access controls should be reviewed and strictly enforced. A Project Manager like Marvin Jonson should not have had access to, or knowledge of, shared developer credentials in the first place.

Improve Technical Threat Detection and Response:
To quickly detect and respond to threats that bypass initial defenses, I recommend the following technical controls:

- **Endpoint Detection and Response (EDR):** A modern EDR solution would have provided critical visibility into the malicious activity on Jonson's workstation. It could have detected and blocked the execution of the keylogger (akl.exe) and alerted security teams to the creation of persistence via a Scheduled Task and the unauthorized modification of firewall rules.

- **Data Loss Prevention (DLP) System:** A DLP solution on email gateways and endpoints would automatically identify and block the exfiltration of sensitive information, such as the credentials sent by Jonson and the Games.zip file he sent as an attachment.

- **Insider Threat Monitoring:** A formal insider threat program, using User and Entity Behavior Analytics (UEBA), would baseline normal user activity. This would help flag high risk anomalies like a project manager suddenly installing unauthorized software , modifying security settings , and emailing sensitive files externally.

Conclusion

The investigation into the Giggly Goofo security incident reveals a deliberate and highly targeted attack that combined coercion, social engineering, and insider collaboration. An external threat actor, identified as "Dr. Evil," contacted Project Manager Marvin Jonson, issuing threats and exerting pressure that compelled Jonson to act on the actor’s behalf. This coercion transformed Jonson into an unwitting insider threat, providing the actor with trusted internal access.

The attack began when Jonson, under duress, transmitted confidential FTP credentials (GigglyGoofoDev) to the actor. From an external IP address (157.165.0.25), the actor leveraged these credentials to access the company's FTP server and exfiltrate proprietary game development files. The compromise escalated as Jonson, following explicit instructions, installed a keylogger on his workstation, created a scheduled task to maintain persistence, and modified local firewall rules to facilitate ongoing malware operations.

Analysis indicates the root cause was human exploitation rather than a technical vulnerability. Network logs, email records, and system artifacts provide a clear and comprehensive timeline of the events. The immediate impact included the confirmed theft of intellectual property and the establishment of a persistent threat on a single workstation. No evidence was found indicating lateral movement beyond the initial host.

The strategic recommendations previously outlined remain essential to remediate procedural and technical weaknesses that enabled this human centric attack, emphasizing the need for controls against both social engineering and insider threats.