Moonstone Sleet emerges as new North Korean threat actor with new bag of tricks

⋮ 5/28/2024

Microsoft has identified a new North Korean threat actor, now tracked as Moonstone Sleet (formerly Storm-1789), that uses both a combination of many tried-and-true techniques used by other North Korean threat actors and unique attack methodologies to target companies for its financial and cyberespionage objectives. Moonstone Sleet is observed 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.

DeTankWar

Malicious tank game

Moonstone Sleet uses tactics, techniques, and procedures (TTPs) also used by other North Korean threat actors over the last several years, highlighting the overlap among these groups. While Moonstone Sleet initially had overlaps with Diamond Sleet, the threat actor has since shifted to its own infrastructure and attacks, establishing itself as a distinct, well-resourced North Korean threat actor.

FakePenny

Moonstone Sleet ransomware

This blog describes several notable TTPs used by this threat actor as well as recommendations to defend against related attacks. As with any observed nation-state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the necessary information to secure their environments.

PROTECTION INFO

Get mitigation, detection, and hunting guidance

Who is Moonstone Sleet?

Moonstone Sleet is a threat actor behind a cluster of malicious activity that Microsoft assesses is North Korean state-aligned and uses both a combination of many tried-and-true techniques used by other North Korean threat actors and unique attack methodologies. When Microsoft first detected Moonstone Sleet activity, the actor demonstrated strong overlaps with Diamond Sleet, extensively reusing code from known Diamond Sleet malware like Comebacker and using well-established Diamond Sleet techniques to gain access to organizations, such as using social media to deliver trojanized software. However, Moonstone Sleet quickly shifted to its own bespoke infrastructure and attacks. Subsequently, Microsoft has observed Moonstone Sleet and Diamond Sleet conducting concurrent operations, with Diamond Sleet still utilizing much of its known, established tradecraft.

Moonstone Sleet has an expansive set of operations supporting its financial and cyberespionage objectives. These range from deploying custom ransomware to creating a malicious game, setting up fake companies, and using IT workers.

Moonstone Sleet tradecraft

Microsoft has observed Moonstone Sleet using the TTPs discussed in the following sections in various campaigns.

Trojanized PuTTY

In early August 2023, Microsoft observed Moonstone Sleet delivering a trojanized version of PuTTY, an open-source terminal emulator, via apps like LinkedIn and Telegram as well as developer freelancing platforms. Often, the actor sent targets a *.zip* archive containing two files: a trojanized version of *putty.exe* and *url.txt*, which contained an IP address and a password. If the provided IP and password were entered by the user into the PuTTY application, the application would decrypt an embedded payload, then load and execute it. Notably, before Moonstone Sleet used this initial access vector, Microsoft observed Diamond Sleet using a similar method – trojanized PuTTY and SumatraPDF — with comparable techniques for anti-analysis, as we reported in 2022:

```
lpPassword = *(const char **)(lpInputObj - 288);
if ( !strcmp(lpPassword, "LH2MStEgzesQPNwa") )
{
  *(_QWORD *)(lpInputObj - 288) = f_gen_pwd_buffer("FG6pEqFe5:b$Bzt");// replace pwd buffer
  nSizeDecompressed.m128i_i32[0] = 0x1D2338;
  lpPePayload = LocalAlloc(0x40u, 0x1D2338ui64);
  strcpy(keyBuff, "6x6s+>e:j~SVK9_0V?m;=Obxd=n+5%-@");
  f_crypt_payload(
    (unsigned int)keyBuff,
    (unsigned int)keyBuff,
    (unsigned int)&crypt_buffer,
    (unsigned int)&crypt_buffer,
    0x2E9ECi64);
  if ( !(unsigned int)f_zlib_decompress(lpPePayload, &nSizeDecompressed, &crypt_buffer, 0x2E9ECi64)
    && f_load_exec_pe_payload(lpPePayload) == -1 )
  {
    LocalFree(lpPePayload);
  }
}
else if ( !strcmp(lpPassword, "FG6pEqFe5:b$Bzt") )
{
  *(_QWORD *)(lpInputObj - 288) = f_gen_pwd_buffer("LH2MStEgzesQPNwa");// replace pwd buffer
}
```

Figure 1. Code from PuTTY executable

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.

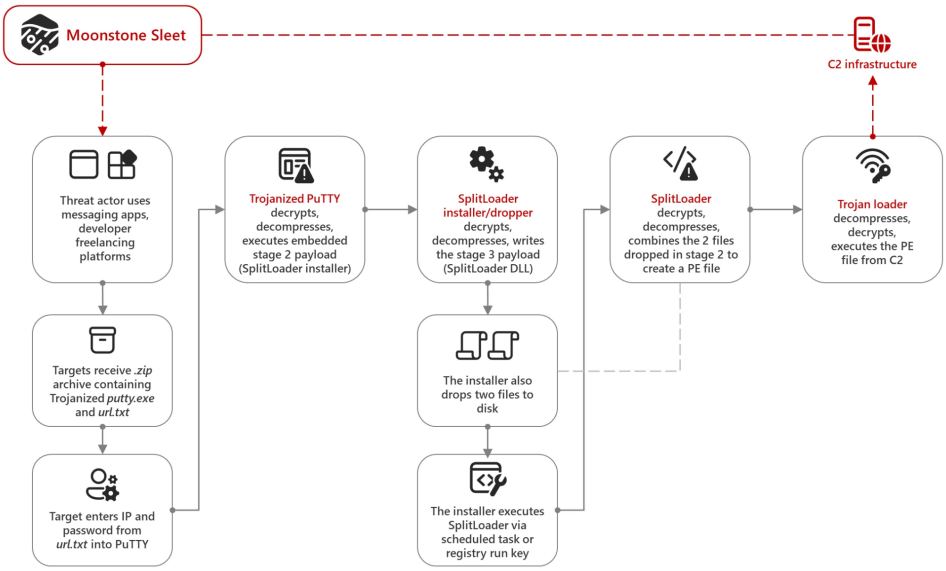

Figure 2. Moonstone Sleet attack chain using trojanized PuTTY

Microsoft has also observed Moonstone Sleet using other custom malware loaders delivered by PuTTY that behaved similarly and had argument overlap with previously observed Diamond Sleet malware artifacts, such as the following:

```
cmd /c C:\ProgramData\USOShared\adb.bin 62
C:\ProgramData\USOShared\uso.bin SmLLPPZLb2vjue3d
```

Malicious npm packages

Microsoft has observed Moonstone Sleet targeting potential victims with projects that used malicious npm packages. Often, the threat actor delivered these projects through freelancing websites or other platforms like LinkedIn. In one example, the threat actor used a fake company to send *.zip* files invoking a malicious npm package under the guise of a technical skills assessment. When loaded, the malicious package used *curl* to connect to an actor-controlled IP and drop additional malicious payloads like SplitLoader. In another incident, Moonstone Sleet delivered a malicious npm loader which led to credential theft from LSASS. Microsoft collaborated with GitHub to identify and remove repositories associated with this activity.

Malicious tank game

Since February 2024, Microsoft has observed Moonstone Sleet infecting devices using a malicious tank game it developed called DeTankWar (also called DeFiTankWar, DeTankZone, or TankWarsZone). DeTankWar is a fully functional downloadable game that requires player registration, including username/password and invite code. In this

campaign, Moonstone Sleet typically approaches its targets through messaging platforms or by email, presenting itself as a game developer seeking investment or developer support and either masquerading as a legitimate blockchain company or using fake companies. To bolster the game's superficial legitimacy, Moonstone Sleet has also created a robust public campaign that includes the websites *detankwar[.]com* and *defitankzone[.]com*, and many X (Twitter) accounts for the personas it uses to approach targets and for the game itself.

Figure 3. Example of a Moonstone Sleet X (Twitter) account for its DeTankWar game

Moonstone Sleet used a fake company called C.C. Waterfall to contact targets. The email presented the game as a blockchain-related project and offered the target the opportunity to collaborate, with a link to download the game included in the body of the message. More details about C.C. Waterfall and another fake company that Moonstone Sleet set up to trick targets are included below:

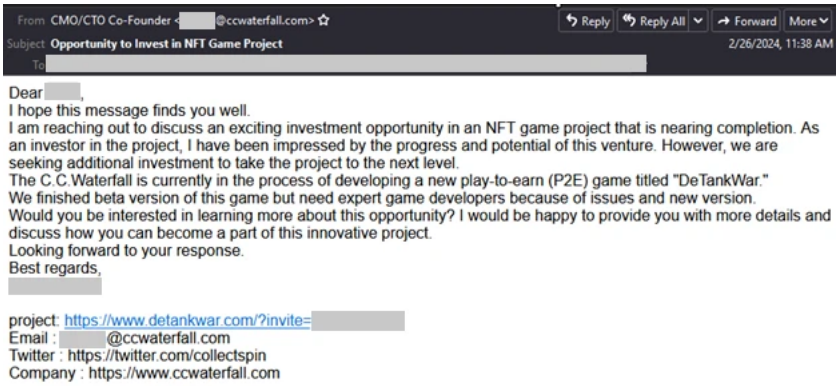

Figure 4. Moonstone Sleet using CC Waterfall to email a link to their game

When targeted users launch the game, *delfi-tank-unity.exe,* additional included malicious DLLs are also loaded. The payload is a custom malware loader that Microsoft tracks as YouieLoad. Similarly to SplitLoader, YouieLoad loads malicious payloads in memory and creates malicious services that perform functions such as network and user discovery and browser data collection. For compromised devices of particular interest to the group, the threat actor launches hands-on-keyboard commands with further discovery and conducts credential theft.

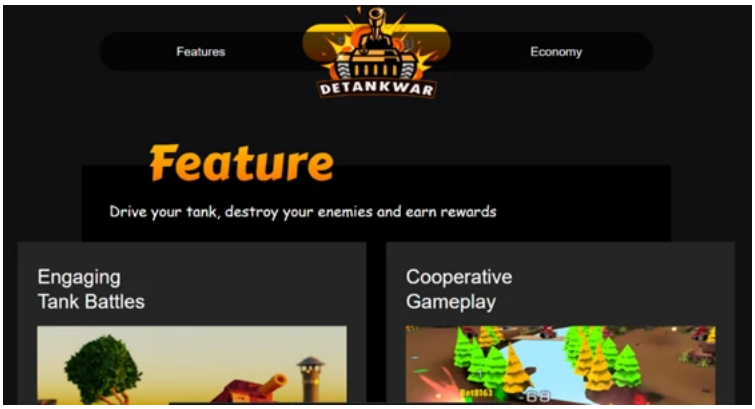

Figure 5. Page from the DeTankWar website

Ransomware

RANSOMWARE AND EXTORTION

Learn how you can better protect your organization

In April 2024, Microsoft observed Moonstone Sleet delivering a new custom ransomware variant we have named FakePenny against a company it previously compromised in February. FakePenny includes a loader and an encryptor. Although North Korean threat actor groups have previously developed custom ransomware, this is the first time we have observed this threat actor deploying ransomware.

Microsoft assesses that Moonstone Sleet's objective in deploying the ransomware is financial gain, suggesting the actor conducts cyber operations for both intelligence collection and revenue generation. Of note, the ransomware note dropped by FakePenny closely overlaps with the note used by Seashell Blizzard in its malware NotPetya. The ransom demand was $6.6M USD in BTC. This is in stark contrast to the lower ransom demands of previous North Korea ransomware attacks, like WannaCry 2.0 and H0lyGh0st.

Figure 6. FakePenny ransomware note

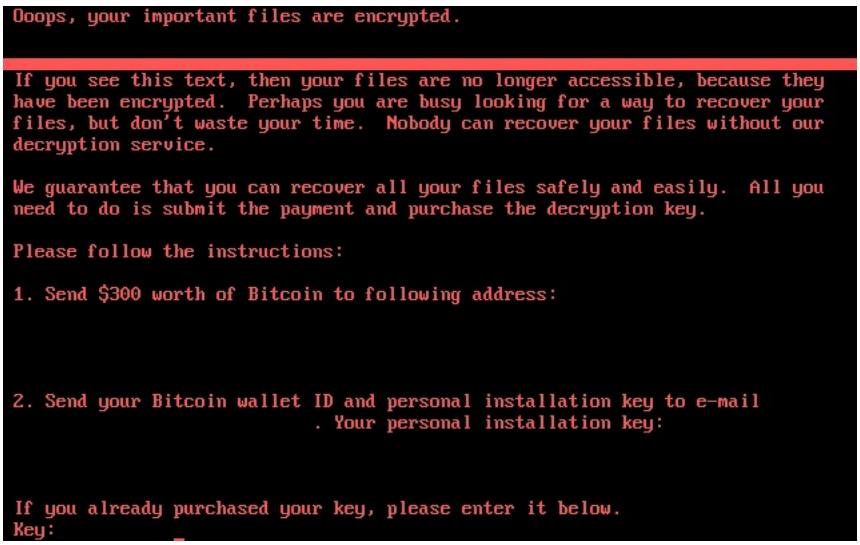

Figure 7. NotPetya ransomware note

Fake companies

Since January 2024, Microsoft has observed Moonstone Sleet creating several fake companies impersonating software development and IT services, typically relating to blockchain and AI. The actor has used these companies to reach out to potential targets, using a combination of created websites and social media accounts to add legitimacy to their campaigns.

StarGlow Ventures

From January to April 2024, Moonstone Sleet's fake company StarGlow Ventures posed as a legitimate software development company. The group used a custom domain, fake employee personas, and social media accounts, in an email campaign targeting thousands of organizations in the education and software development sectors. In the

emails Moonstone Sleet sent as part of this campaign, the actor complimented the work of the targeted organization and offered collaboration and support for upcoming projects, citing expertise in the development of web apps, mobile apps, blockchain, and AI.

Figure 8. Example of an email from Moonstone Sleet's StarGlow Ventures campaign

These emails also contained a 1×1 tracking pixel, which likely enabled Moonstone Sleet to track which targets engaged with the emails, and a link to a dummy unsubscribe page hosted on the StarGlow Ventures domain. While the emails did not contain any malicious links, Microsoft assesses Moonstone Sleet likely used this campaign to establish a relationship with target organizations. Although the purpose of these relationships is unclear, they may afford the actor access to organizations of interest or be used as revenue generation opportunities. Microsoft notified customers who were impacted by this Moonstone Sleet campaign.

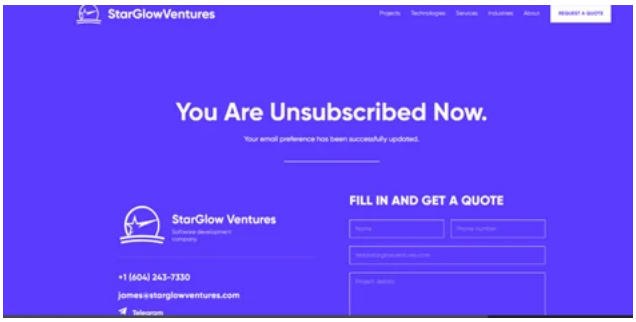

Figure 9. Unsubscribe page on the StarGlow Ventures website

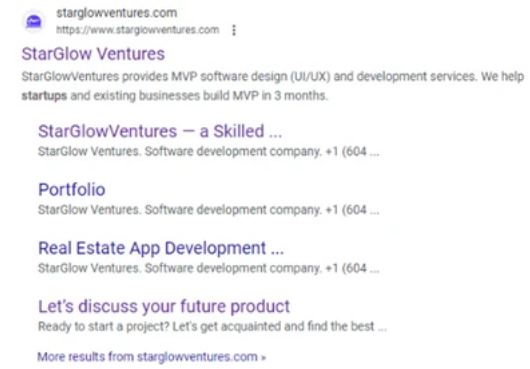

Figure 10. Informational pages for the StarGlow Ventures website

C.C. Waterfall

In a similar campaign, Moonstone Sleet sent emails using its fake company C.C. Waterfall, a purported IT consulting organization.

Figure 11. The landing page for C.C. Waterfall

In this campaign, Moonstone Sleet emailed higher education organizations, claiming the company was either hiring new developers or looking for business collaboration opportunities. This campaign likely had similar goals to the StarGlow Ventures campaign: to build relationships with organizations which could be leveraged for revenue generation or malicious access.


P1Sender
P2Sender @ccwaterfall.com>
Subject Job or contract part-time role opportunity
Recipient
ReportHeader
Message-Id
Hello,
This is from CCWaterfall, IT consultant company.
I checked your profile and I am interested.

Now we are hiring Python developer.

if you are not interested for a new role, new position, we can discuss about business partnership or development collaboration.

If you are interested in this role, we can discuss more about project on chatting or interview.

telegram : https://t.me/mrsafdarmanager
email : @ccwaterfall.com

Figure 12. Example of an email from C.C. Waterfall

As previously mentioned, Moonstone Sleet also used C.C. Waterfall to contact targets and invite them to download the actor's tank game, highlighting that this is a coordinated and concerted effort for which Moonstone Sleet can leverage multiple facets of its operations in overlapping campaigns.

Work-for-hire

In addition to creating fake companies, Microsoft has observed Moonstone Sleet pursuing employment in software development positions at multiple legitimate companies. This activity could be consistent with previous reporting from the United States Department of Justice that North Korea was using highly skilled remote IT workers to generate revenue. On the other hand, this Moonstone Sleet activity may also be another approach to gaining access to organizations.

Moonstone Sleet targets

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 the above 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 via 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.

Fitting into the North Korean threat actor landscape

Sleet Actors

Read about North Korean threat actors

Moonstone Sleet's diverse set of tactics is notable not only because of their effectiveness, but because of how they have evolved from those of several other North Korean threat actors over many years of activity to meet North Korean cyber objectives. For example, North Korea has for many years maintained a cadre of remote IT workers to

generate revenue in support of the country's objectives. Moonstone Sleet's pivot to conduct IT work within its campaigns indicates it may not only be helping with this strategic initiative, but possibly also expanding the use of remote IT workers beyond just financial gain. Additionally, Moonstone Sleet's addition of ransomware to its playbook, like another North Korean threat actor, Onyx Sleet, may suggest it is expanding its set of capabilities to enable disruptive operations. Microsoft reported on Onyx Sleet's and Storm-0530's h0lyGhost ransomware in 2022.

Moonstone Sleet's ability to conduct concurrent operations across multiple campaigns, the robustness of the malicious game, and the use of a custom new ransomware variant are strong indications that this threat actor may be well-resourced. Moreover, given that Moonstone Sleet's initial attacks mirrored Diamond Sleet methodologies and heavily reused Diamond Sleet's code in their payloads, Microsoft assesses this actor is equipped with capabilities from prior cyber operations conducted by other North Korean actors.

Microsoft has identified several techniques used by Moonstone Sleet that have previously been used by other North Korean threat actors. For example, since late 2023, an actor that Microsoft tracks as Storm-1877 used malicious npm packages in a campaign targeting software developers with JavaScript-based malware. This campaign was reported publicly by PaloAlto as Contagious Interview. Additionally, in 2023, GitHub reported that Jade Sleet used malicious npm packages in a campaign consisting of fake developer and recruiter personas that operated on LinkedIn, Slack, and Telegram. This shared use of a relatively uncommon tactic across multiple distinct North Korean groups may suggest sharing of expertise and TTPs among North Korean threat actors.

In recent months, Microsoft and other security researchers have reported on North Korean threat actors' use of software supply chain attacks to conduct widespread malicious operations. In November 2023, Microsoft reported on Diamond Sleet's supply chain compromise of CyberLink, a multimedia application. While Microsoft has not yet identified any Moonstone Sleet supply chain attacks, the actor has extensively targeted software development firms in its campaigns. Large-scale access to software companies would pose a particularly high risk for future supply chain attacks against those organizations.

Moonstone Sleet's appearance is an interesting development considering that North Korea has carried out a series of changes in its foreign relations and security apparatus. In November 2023, North Korea closed embassies in several countries, and in March 2024, may have dissolved the United Front Department (UFD), an agency believed to be responsible for reunification and propaganda.

Despite being new, Moonstone Sleet has demonstrated that it will continue to mature, develop, and evolve, and has positioned itself to be a preeminent threat actor conducting sophisticated attacks on behalf of the North Korean regime.

Recommendations

Microsoft recommends the following mitigations defend against attacks by Moonstone Sleet:

- Detect human-operated ransomware attacks with Microsoft Defender XDR.
- Enable controlled folder access.
- Ensure that tamper protection is enabled in Microsoft Dender for Endpoint.
- Enable network protection in Microsoft Defender for Endpoint.
- Follow the credential hardening recommendations in our on-premises credential theft overview to defend against common credential theft techniques like LSASS access.
- Run endpoint detection and response (EDR) in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Configure investigation and remediation in full automated mode to let Microsoft Defender for Endpoint take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus, or the equivalent for your antivirus product, to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a majority of new and unknown variants.

Microsoft Defender XDR customers can turn on the following attack surface reduction rule to prevent common attack techniques used by Moonstone Sleet.

- Block executable content from email client and webmail
- Block executable files from running unless they meet a prevalence, age, or trusted list criterion
- Use advanced protection against ransomware
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)

Detection details

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- Behavior:Win64/PennyCrypt

- HackTool:Win32/Mimikatz
- HackTool:Win64/Mimikatz
- TrojanDropper:Win32/SplitLoader
- TrojanDropper:Win64/YouieLoad

Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate threat activity on your network:

- Moonstone Sleet actor activity detected
- Suspicious activity linked to a North Korean state-sponsored threat actor has been detected
- Diamond Sleet Actor activity detected

The following alerts might also indicate threat activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity and are not monitored in the status cards provided with this report.

- Malicious credential theft tool execution detected
- Mimikatz credential theft tool
- Ransomware-linked threat actor detected
- Suspicious access to LSASS service

Hunting queries

Microsoft Defender XDR

Microsoft Defender XDR customers can run the following query to find related activity in their networks:

Detect Procdump dumping LSASS credentials:

```
DeviceProcessEvents

| where (FileName has_any ("procdump.exe",

"procdump64.exe") and ProcessCommandLine has "lsass") or

(ProcessCommandLine

has "lsass.exe" and (ProcessCommandLine has "-accepteula"

or ProcessCommandLine contains "-ma"))
```

Detect connectivity with C2 infrastructure:

```
let c2servers = dynamic(['mingeloem.com','matrixane.com']);

DeviceNetworkEvents

| where RemoteUrl has_any (c2servers)

| project DeviceId, LocalIP, DeviceName, RemoteUrl, InitiatingProcessFileName,
InitiatingProcessCommandLine, Timestamp
```

Detect connectivity to DeTank websites:

```
let c2servers = dynamic(['detankwar.com','defitankzone.com']);

DeviceNetworkEvents

| where RemoteUrl has_any (c2servers)

| project DeviceId, LocalIP, DeviceName, RemoteUrl, InitiatingProcessFileName,
InitiatingProcessCommandLine, Timestamp
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with ‘TI map’) to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

Microsoft Sentinel customers can also use the queries below to detect activity detailed in this blog.

This query detects the installation of a Windows service that contains artifacts from credential dumping tools such as Mimikatz:

- Credential Dumping Tools – Service Installation

This query detects the use of Procdump to dump credentials from LSASS memory:

- Dump credential using procdump

Microsoft Sentinel customers can also use the following query, which looks for Microsoft Defender AV detections related to the Moonstone Sleet. In Microsoft Sentinel, the *SecurityAlerts* table includes only the *DeviceName* of the affected device. This query joins the *DeviceInfo* table to connect other information such as device group, IP, signed-in users, etc., allowing analysts to have more context related to the alert, if available:

```
let MoonStoneSleet_threats = dynamic(["Behavior:Win64/PennyCrypt", "HackTool:Win32/Mimikatz",
"HackTool:Win64/Mimikatz ", "TrojanDropper:Win32/SplitLoader", "TrojanDropper:Win64/YouieLoad" ]);

SecurityAlert

| where ProviderName == "MDATP"

| extend ThreatName = tostring(parse_json(ExtendedProperties).ThreatName)

| extend ThreatFamilyName = tostring(parse_json(ExtendedProperties).ThreatFamilyName)

| where ThreatName in~ (MoonStoneSleet_threats) or ThreatFamilyName in~ (MoonStoneSleet_threats)

| extend CompromisedEntity = tolower(CompromisedEntity)

| join kind=inner (

DeviceInfo

| extend DeviceName = tolower(DeviceName)

) on $left.CompromisedEntity == $right.DeviceName

| summarize arg_max(TimeGenerated, *) by DisplayName, ThreatName, ThreatFamilyName, PublicIP,
AlertSeverity, Description, tostring(LoggedOnUsers), DeviceId, TenantId, CompromisedEntity,
ProductName, Entities

| extend HostName = tostring(split(CompromisedEntity, ".")[0]), DomainIndex =
toint(indexof(CompromisedEntity, '.'))

| extend HostNameDomain = iff(DomainIndex != -1, substring(CompromisedEntity, DomainIndex + 1),
CompromisedEntity)

| project-away DomainIndex

| project TimeGenerated, DisplayName, ThreatName, ThreatFamilyName, PublicIP, AlertSeverity,
Description, LoggedOnUsers, DeviceId, TenantId, CompromisedEntity, ProductName, Entities, HostName,
HostNameDomain
```

Indicators of compromise

Malicious files

File	SHA-256 hash
putty.exe (drops SplitLoader)	f59035192098e44b86c4648a0de4078edbe80352260276f4755d15d354f5fc58
putty.exe (drops SplitLoader)	cb97ec024c04150ad419d1af2d1eb66b5c48ab5f345409d9d791db574981a3fb
[random].dat (SplitLoader)	39d7407e76080ec5d838c8ebca5182f3ac4a5f416ff7bda9cbc4efffd78b4ff5
Package.db, thumbs.db (YouieLoad via npm)	70c5b64589277ace59db86d19d846a9236214b48aacabbaf880f2b6355ab5260
adb.bin, u.bin, ld.bin (YouieLoad)	cafaa7bc3277711509dc0800ed53b82f645e86c195e85fbf34430bbc75c39c24
data.tmp (YouieLoad)	9863173e0a45318f776e36b1a8529380362af8f3e73a2b4875e30d31ad7bd3c1
delfi-tank-unity.exe	f66122a3e1eaa7dcb7c13838037573dace4e5a1c474a23006417274c0c8608be
DeTankWar.exe	56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c ecce739b556f26de07adbfc660a958ba2dca432f70a8c4dd01466141a6551146
NVUnityPlugin.dll, Unityplayer.dll (YouieLoad via tank game)	09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e84a6cc38

Moonstone Sleet domains

bestonlinefilmstudio[.]org
blockchain-newtech[.]com
ccwaterfall[.]com
chaingrown[.]com
defitankzone[.]com
detankwar[.]com
freenet-zhilly[.]org
matrixane[.]com
pointdnt[.]com

starglowventures[.]com
mingeloem[.]com

References

- Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors (Palo Alto Unit 42)
- Security alert: social engineering campaign targets technology industry employees (Github)