Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets

4/18/2023

Over the past several months, Microsoft has observed a mature subgroup of Mint Sandstorm, an Iranian nation-state actor previously tracked as PHOSPHORUS, refining its tactics, techniques, and procedures (TTPs). Specifically, this subset has rapidly weaponized N-day vulnerabilities in common enterprise applications and conducted highly-targeted phishing campaigns to quickly and successfully access environments of interest. This Mint Sandstorm subgroup has also continued to develop and use custom tooling in selected targets, notably organizations in the energy and transportation sectors. Given this subgroup's capabilities, the profile of past targets, and the potential for cascading effects, Microsoft is publishing details on known tradecraft alongside corresponding detections and mitigations to help organizations protect against this and similar threats.

Who is Mint Sandstorm?

Mint Sandstorm is Microsoft's new name for PHOSPHORUS, an Iranian nation-state actor. This new name is part of the new threat actor naming taxonomy we announced today, designed to keep pace with the evolving and growing threat landscape.

Mint Sandstorm is known to pursue targets in both the private and public sectors, including political dissidents, activist leaders, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East. Activity Microsoft tracks as part of the larger Mint Sandstorm group overlaps with public reporting on groups known as APT35, APT42, Charming Kitten, and TA453.

Mint Sandstorm is a composite name used to describe several subgroups of activity with ties to the same organizational structure. Microsoft assesses that Mint Sandstorm is associated with an intelligence arm of Iran's military, the Islamic Revolutionary Guard Corps (IRGC), an assessment that has been corroborated by multiple credible sources including Mandiant, Proofpoint, and SecureWorks. In 2022, the US Department of Treasury sanctioned elements of Mint Sandstorm for past cyberattacks citing sponsorship from the IRGC.

Today, Microsoft is reporting on a distinct Mint Sandstorm subgroup that specializes in hacking into and stealing sensitive information from high-value targets. This Mint Sandstorm subgroup is technically and operationally mature, capable of developing bespoke tooling and quickly weaponizing N-day vulnerabilities, and has demonstrated agility in its operational focus, which appears to align with Iran's national priorities.

Microsoft Threat Intelligence consistently tracks threat actor activity, including Mint Sandstorm and its subgroups, and works across Microsoft Security products and services to build detections into our products that improve protection for customers. As with any observed nation state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the information they need to secure their accounts. Microsoft is sharing details on these operations to raise awareness on the risks associated with their activity and to empower organizations to harden their attack surfaces against tradecraft commonly used by this Mint Sandstorm subgroup.

Recent operations

From late 2021 to mid-2022, this Mint Sandstorm subgroup moved from reconnaissance to direct targeting of US critical infrastructure including seaports, energy companies, transit systems, and a major US utility and gas entity potentially in support of retaliatory destructive cyberattacks. This targeting was likely in response to Iran's attribution of cyberattacks that halted maritime traffic at a major Iranian seaport in May 2020, delayed Iranian trains in July 2021, and crashed gas station payment systems throughout Iran in late 2021. Of note, a senior cybersecurity-focused IRGC official and others close to the Iranian Supreme Leader pinned the attack affecting gas station payment systems on Israel and the United States.

This targeting also coincided with a broader increase in the pace and the scope of cyberattacks attributed to Iranian threat actors, including another Mint Sandstorm subgroup, that Microsoft observed beginning in September 2021. The increased aggression of Iranian threat actors appeared to correlate with other moves by the Iranian regime under a new national security apparatus, suggesting such groups are less bounded in their operations. Given the hardline consensus among policymakers in Tehran and sanctions previously levied on Iran's security organizations, Mint Sandstorm subgroups may be less constrained in carrying out malicious cyber activity.

Mint Sandstorm tradecraft

Microsoft has observed multiple attack chains and various tools in compromises involving this Mint Sandstorm subgroup. The TTPs detailed below are a sampling of new or otherwise notable tradecraft used by this actor.

Rapid adoption of publicly disclosed POCs for initial access and persistence

Microsoft has increasingly observed this Mint Sandstorm subgroup adopting publicly disclosed proof-of-concept (POC) code shortly after it is released to exploit vulnerabilities in internet-facing applications. Until 2023, this subgroup had been slow to adopt exploits for recently-disclosed vulnerabilities with publicly reported POCs, often taking several weeks to successfully weaponize exploits for vulnerabilities like Proxyshell and Log4Shell. However, beginning in early 2023, Microsoft observed a notable decrease in the time required for this subgroup to adopt and incorporate public POCs. For example, Mint Sandstorm began exploiting CVE-2022-47966 in Zoho ManageEngine on January 19, 2023, the same day the POC became public. They later exploited CVE-2022-47986 in Aspera Faspex within five days of the POC being made public on February 2, 2023.

While this subgroup has demonstrated their ability to rapidly incorporate new public POCs into their playbooks, Microsoft has also observed that Mint Sandstorm continues to use older vulnerabilities, especially Log4Shell, to compromise unpatched devices. **As this activity is typically opportunistic and indiscriminate, Microsoft recommends that organizations regularly patch vulnerabilities with publicly available POCs, regardless of how long the POC has been available.**

After gaining initial access to an organization by exploiting a vulnerability with a public POC, this Mint Sandstorm subgroup deploys a custom PowerShell script designed for discovery. In some cases, the subgroup does not act on the information they collect, possibly because they assess that a victim does not meet any targeting requirements or because the subgroup wishes to wait and focus on more valuable targets. In cases where Mint Sandstorm operators continue their pursuit of a given target, Microsoft typically observes one of two possible attack chains.

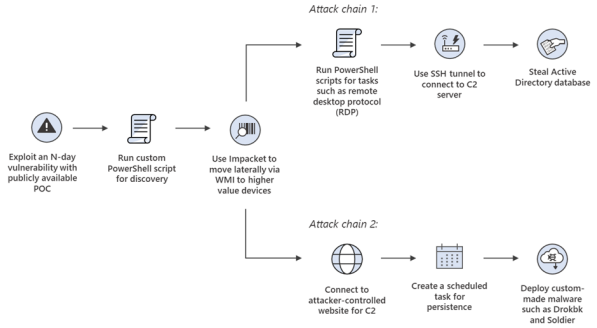

Figure 1. The two attack chains used by the Mint Sandstorm subgroup

- **Attack chain 1:** The Mint Sandstorm subgroup proceeds using Impacket to move laterally through a compromised organization and relies extensively on PowerShell scripts (rather than custom implants) to enumerate admin accounts and enable RDP connections. In this attack chain, the subgroup uses an SSH tunnel for command and control (C2), and the final objective in many cases is theft of the Active Directory database. If obtained, the Mint Sandstorm subgroup can use the Active Directory database to access credentials for users' accounts. In cases where users' credentials are accessed and the target organization has not reset corresponding passwords, the actors can log in with stolen credentials and masquerade as legitimate users, possibly without attracting attention from defenders. The actors could also gain access to other systems where individuals may have reused their passwords.
- **Attack chain 2**: As is the case in attack chain 1, the Mint Sandstorm subgroup uses Impacket to move laterally. However, in this progression, the operators use *webhook.site* for C2 and create scheduled tasks for persistence. Finally, in this attack chain, the actors deploy a custom malware variant, such as Drokbk or Soldier. These custom malware variants signal an increase in the subgroup's level of sophistication, as they shift from using publicly available tools and simple scripts to deploying fully custom developed malicious code.

Use of custom tools to evade detection

Since 2022,Microsoft has observed this Mint Sandstorm subgroup using two custom implants, detected by Microsoft security products as Drokbk and Soldier, to persist in target environments and deploy additional tools. Drobkbk and Soldier both use Mint Sandstorm-controlled GitHub repositories to host a domain rotator containing the operators' C2 domains. This allows Mint Sandstorm to dynamically update their C2 infrastructure, which may help the operators stay a step ahead of defenders using list-based domain blocking.

- **Drokbk**: *Drokbk.exe* is a custom .NET implant with two components: an installer, sometimes accessed from a compressed archive on a legitimate file-sharing platform, and a secondary backdoor payload. The Drokbk backdoor issues a web request to obtain the contents of a *README* file on a Mint Sandstorm-controlled GitHub repo. The *README* file contains a list of URLs that direct targets to the C2 infrastructure associated with Drokbk.
- **Soldier:** Soldier is a multistage .NET backdoor with the ability to download and run additional tools and uninstall itself. Like Drokbk, Soldier C2 infrastructure is stored on a domain rotator on a GitHub repository operated by Mint Sandstorm. Microsoft Threat Intelligence analysts assess that Soldier is a more sophisticated variant of Drokbk.

In certain cases, this Mint Sandstorm subgroup has used TTPs outside of these attack chains, notably when they have failed to achieve short-term objectives. In one instance, Microsoft also observed the subgroup using TTPs from both attack chains in a single compromised environment. However, in most cases, Mint Sandstorm activity displays one of the above discussed attack chains.

Low-volume phishing campaigns using template injection

Microsoft has also observed this Mint Sandstorm subgroup using a distinct attack chain involving low-volume phishing campaigns and a third custom implant.In these operations, the group crafts bespoke phishing emails, often purporting to contain information on security policies that affect countries in the Middle East, to deliver weaponized documents to individuals of interest. Recipients are typically individuals affiliated with high-profile think tanks or universities in Israel, North America, or Europe with ties to the security and policy communities. Unlike their initial

exploitation of vulnerable internet-facing applications, which is largely indiscriminate and affects organizations across sectors and geographies, activity associated with this campaign was highly targeted and affected fewer than 10 organizations..

The initial emails are most commonly lures designed to social engineer recipients into clicking a OneDrive link hosting a PDF spoofed to resemble information on a topic involving security or policy in the Middle East. The PDF contains a link to a macro-enabled template file (dotm) hosted on Dropbox. This file has been weaponized with macros to perform remote template injection, a technique that allows operators to obtain and launch a payload from a remote C2, often OneDrive. Template injection is an attractive option for adversaries looking to execute malicious code without drawing scrutiny from defenders. This technique can also be used to persist in a compromised environment if an adversary replaces a default template used by a common application.

In these attacks, Microsoft has observed the Mint Sandstorm subgroup using CharmPower, a custom implant, in attacks that began with targeted phishing campaigns.CharmPower is a modular backdoor written in PowerShell that this subgroup delivers in phishing campaigns that rely on template injection. CharmPower can read files, gather information on an infected host, and send details back to the attackers. Reporting from Checkpoint indicates that at least one version of CharmPower pulls data from a specific text file that contains a hardcoded victim identifier.

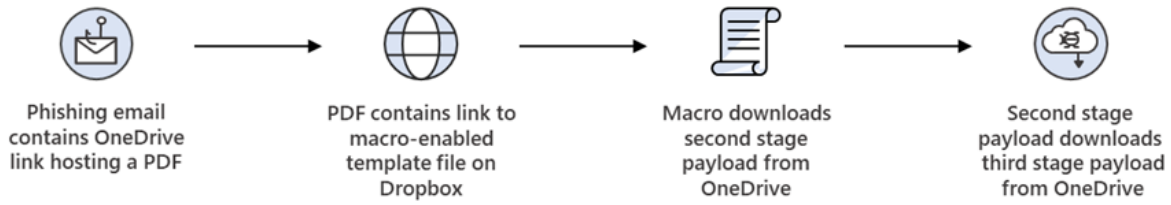

Figure 2. Template injection technique

What's next

Capabilities observed in intrusions attributed to this Mint Sandstorm subgroup are concerning as they allow operators to conceal C2 communication, persist in a compromised system, and deploy a range of post-compromise tools with varying capabilities. While effects vary depending on the operators' post-intrusion activities, even initial access can enable unauthorized access and facilitate further behaviors that may adversely impact the confidentiality, integrity, and availability of an environment. A successful intrusion creates liabilities and may harm an organization's reputation, especially those responsible for delivering services to others such as critical infrastructure providers, which Mint Sandstorm has targeted in the past.

As these operators increasingly develop and use sophisticated capabilities, organizations must develop corresponding defenses to harden their attack surfaces and raise costs for these operators. Microsoft will continue to monitor Mint Sandstorm activity and implement protections for our customers. The current detections, advanced detections, and IOCs in place across our security products are detailed below and shared with the broader security community to help detect and prevent further attacks.

Mitigation and protection guidance

The techniques used by this subset of Mint Sandstorm can be mitigated through the following actions:

Hardening internet-facing assets and understanding your perimeter

Organizations must identify and secure perimeter systems that attackers might use to access the network. Public scanning interfaces, such as Microsoft Defender External Attack Surface Management, can be used to improve data.

Vulnerabilities observed in recent campaigns attributed to this Mint Sandstorm subgroup that defenders can identify and mitigate include:

- IBM Aspera Faspex affected by CVE-2022-47986: Organizations can remediate CVE-2022-47986 by upgrading to Faspex 4.4.2 Patch Level 2 or using Faspex 5.x which does not contain this vulnerability. More details are available in IBM's security advisory here.

- Zoho ManageEngine affected by CVE-2022-47966: Organizations using Zoho ManageEngine products vulnerable to CVE-2022-47966 should download and apply upgrades from the official advisory as soon as possible. Patching this vulnerability is useful beyond this specific campaign as several adversaries are exploiting CVE-2022-47966 for initial access.
- Apache Log4j2 (aka Log4Shell) (CVE-2021-44228 and CVE-2021-45046): Microsoft's guidance for organizations using applications vulnerable to Log4Shell exploitation can be found here. This guidance is useful for any organization with vulnerable applications and useful beyond this specific campaign, as several adversaries exploit Log4Shell to obtain initial access.

This Mint Sandstorm subgroup has demonstrated its ability to rapidly adopt newly reported N-day vulnerabilities into its playbooks. To further reduce organizational exposure, Microsoft Defender for Endpoint customers can use the threat and vulnerability management capability to discover, prioritize, and remediate vulnerabilities and misconfigurations.

Reducing the attack surface

Microsoft 365 Defender customers can also turn on attack surface reduction rules to harden their environments against techniques used by this Mint Sandstorm subgroup. These rules, which can be configured by all Microsoft Defender Antivirus customers and not just those using the EDR solution, offer significant protection against the tradecraft discussed in this report.

- Block executable files from running unless they meet a prevalence, age, or trusted list criterion
- Block Office applications from creating executable content
- Block process creations originating from PSExec and WMI commands

Additionally, in 2022, Microsoft changed the default behavior of Office applications to block macros in files from the internet, further minimizing the attack surface for operators like this subgroup of Mint Sandstorm.

Microsoft 365 Defender detections

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects the Drokbk implant as the following malware:

- Trojan:MSIL/Drokbk.A!dha
- Trojan:MSIL/Drokbk.B!dha
- Trojan:MSIL/Drokbk.C!dha
- Trojan:Win32/Drokbk.C!dha

Microsoft Defender Antivirus detects the Soldier implant as the following malware:

- Trojan:MSIL/SoldierAudio.A!dha
- Trojan:MSIL/SoldierAudio.B!dha
- Trojan:MSIL/SoldierAudio.C!dha

Microsoft Defender Antivirus detects the CharmPower implant as the following malware:

- TrojanDownloader:O97M/RooftopMelt.A!dha

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alerts can indicate associated threat activity:

- Phosphorus Actor activity detected

Hunting queries

Microsoft 365 Defender

Microsoft 365 Defender customers can run the following query to find related activity in their networks:

ManageEngine Suspicious Process Execution.

```
DeviceProcessEvents
| where InitiatingProcessFileName hasprefix "java"
| where InitiatingProcessFolderPath  has @"\manageengine\" or
InitiatingProcessFolderPath has @"\ServiceDesk\"
| where (FileName in~ ("powershell.exe", "powershell_ise.exe") and
            (ProcessCommandLine has_any ("whoami", "net user", "net group",
"localgroup administrators", "dsquery", "samaccountname=", " echo ", "query session",
"adscredentials", "o365accountconfiguration", "-dumpmode", "-ssh", "usoprivate",
"usoshared", "Invoke-Expression", "DownloadString", "DownloadFile",
"FromBase64String",  "System.IO.Compression", "System.IO.MemoryStream", "iex ",
"iex(", "Invoke-WebRequest", "set-MpPreference", "add-MpPreference", "certutil",
"bitsadmin") // "csvhost.exe", "ekern.exe", "svhost.exe", ".dmp"
             or ProcessCommandLine matches regex @"[-/-][Ee^]{1,2}[ncodema^]*\s[A-Za-
z0-9+/=]{15,}"))
           or (FileName =~ "curl.exe" and ProcessCommandLine contains "http")
           or (FileName =~ "wget.exe" and ProcessCommandLine contains "http")
           or ProcessCommandLine has_any ("E:jscript", "e:vbscript")
           or ProcessCommandLine has_all ("localgroup Administrators", "/add")
           or ProcessCommandLine has_all ("reg add", "DisableAntiSpyware",
@"\Microsoft\Windows Defender")
           or ProcessCommandLine has_all ("reg add", "DisableRestrictedAdmin",
@"CurrentControlSet\Control\Lsa")
           or ProcessCommandLine has_all ("wmic", "process call create")
           or ProcessCommandLine has_all ("net", "user ", "/add")
           or ProcessCommandLine has_all ("net1", "user ", "/add")
           or ProcessCommandLine has_all ("vssadmin", "delete", "shadows")
           or ProcessCommandLine has_all ("wmic", "delete", "shadowcopy")
           or ProcessCommandLine has_all ("wbadmin", "delete", "catalog")
           or (ProcessCommandLine has "lsass" and ProcessCommandLine has_any
("procdump", "tasklist", "findstr"))
 | where ProcessCommandLine !contains "download.microsoft.com" and ProcessCommandLine
!contains "manageengine.com" and ProcessCommandLine !contains "msiexec"
```

Ruby AsperaFaspex Suspicious Process Execution.

```
DeviceProcessEvents
| where InitiatingProcessFileName hasprefix "ruby"
| where InitiatingProcessFolderPath has @"aspera"
| where (FileName in~ ("powershell.exe", "powershell_ise.exe") and
            (ProcessCommandLine has_any ("whoami", "net user", "net group",
"localgroup administrators", "dsquery", "samaccountname=", " echo ", "query session",
"adscredentials", "o365accountconfiguration", "-dumpmode", "-ssh", "usoprivate",
"usoshared", "Invoke-Expression", "DownloadString", "DownloadFile",
"FromBase64String",  "System.IO.Compression", "System.IO.MemoryStream", "iex ",
"iex(", "Invoke-WebRequest", "set-MpPreference", "add-MpPreference", "certutil",
"bitsadmin", "csvhost.exe", "ekern.exe", "svhost.exe", ".dmp")
             or ProcessCommandLine matches regex @"[-/-][Ee^]{1,2}[ncodema^]*\s[A-Za-
z0-9+/=]{15,}"))
           or (FileName =~ "curl.exe" and ProcessCommandLine contains "http")
           or (FileName =~ "wget.exe" and ProcessCommandLine contains "http")
           or ProcessCommandLine has_any ("E:jscript", "e:vbscript")
           or ProcessCommandLine has_all ("localgroup Administrators", "/add")
           or ProcessCommandLine has_all ("reg add", "DisableAntiSpyware",
@"\Microsoft\Windows Defender")
           or ProcessCommandLine has_all ("reg add", "DisableRestrictedAdmin",
@"CurrentControlSet\Control\Lsa")
```

```
            or ProcessCommandLine has_all ("wmic", "process call create")
            or ProcessCommandLine has_all ("net", "user ", "/add")
            or ProcessCommandLine has_all ("net1", "user ", "/add")
            or ProcessCommandLine has_all ("vssadmin", "delete", "shadows")
            or ProcessCommandLine has_all ("wmic", "delete", "shadowcopy")
            or ProcessCommandLine has_all ("wbadmin", "delete", "catalog")
            or (ProcessCommandLine has "lsass" and ProcessCommandLine has_any
("procdump", "tasklist", "findstr"))
```

Log4J Wstomcat Process Execution.

```
DeviceProcessEvents
| where InitiatingProcessFileName has "ws_tomcatservice.exe" and FileName !in~
("repadmin.exe")
```

Encoded watcher Function.

```
DeviceProcessEvents
| where FileName =~ "powershell.exe" and ProcessCommandLine hasprefix "-e"
| extend SplitString = split(ProcessCommandLine, " ")
| mvexpand SS = SplitString
| where SS matches regex "^[A-Za-z0-9+/]{50,}[=]{0,2}$"
| extend base64_decoded = replace(@'\0', '',
make_string(base64_decode_toarray(tostring(SS))))
| where not(base64_decoded has_any(@"software\checker", "set folder to watch"))
| where base64_decoded has_all("$hst", "$prt") or base64_decoded has_any("watcher",
@"WAt`CH`Er()")
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytic (a series of analytics all prefixed with “TI map”) to automatically match the 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. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy

In addition, Microsoft Sentinel customers can leverage the following content to hunt for and detect related activity in their environments:

Indicators of compromise

Indicator	Type	Description
Soldier.exe	File name	Soldier backdoor
ad55b4a40f9e52682d9d4f069914e09c941e8b77ca7b615e9deffccdfbc54145	SHA-256	Soldier backdoor hash
Drokbk.exe	File name	Drokbk backdoor
64f39b858c1d784df1ca8eb895ac7eaf47bf39acf008ed4ae27a796ac90f841b	SHA-256	Drokbk backdoor hash
sync-system-time[.]cf	Domain	Drokbk C2 infrastructur
update-windows-security[.]tk	Domain	Drokbk C2 infrastructur
dns-iprecords[.]tk	Domain	Drokbk C2 infrastructur
universityofmhealth[.]biz	Domain	Drokbk C2 infrastructur
oracle-java[.]cf	Domain	Drokbk C2 infrastructur
54.39.202[.]0	IP address	Drokbk C2 infrastructur
51.89.135[.]15	IP address	Drokbk C2 infrastructur
51.89.169[.]201	IP	Drokbk C2 infrastructur

	address	
51.89.187[.]222	IP address	Drokbk C2 infrastructur
NY.docx.docx	File name	CharmPower lure docu used for template inject
57cc5e44fd84d98942c45799f367db78adc36a5424b7f8d9319346f945f64a72	SHA-256	NY.docx.docx hash
Abraham%20Accords%20Du.[.]docx	File name	CharmPower lure docu used for template inject
3dcdb0ffebc5ce6691da3d0159b5e811c7aa91f6d8fc204963d2944225b0119d	SHA-256	Abraham%20Accords% [.]docx hash
DocTemplate.dotm	File name	Malicious remote templ document used in intru involving CharmPower
65e48f63f455c94d3bf681acaf115caa6e1e60499362add49ca614458bbc4f85	SHA-256	DocTemplate.dotm
DntDocTemp.dotm	File name	Malicious remote templ document used in intru involving CharmPower
444075183ff6cae52ab5b93299eb9841dcd8b0321e3a90fb29260dc12133b6a2	SHA-256	DntDocTemp.dotm hasl
0onlyastep0[.]xyz	Domain	CharmPower C2 infrastructure
0readerazone0[.]xyz	Domain	CharmPower C2 infrastructure
0tryamore0[.]xyz	Domain	CharmPower C2 infrastructure

References

Iran: Background and U.S. Policy. Congressional Research Service

Cobalt Illusion Masquerades as Atlantic Council Employee. Secureworks

Apt42: Crooked Charms, Cons, and Compromises. Mandiant

Badblood: TA453 Targets US & Israel in Credential Phishing. Proofpoint

Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity. U.S. Department of the Treasury

Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility. The Washington Post

Iran Says Cyberattack Causes Widespread Disruption at Gas Stations. Thomson Reuters

Iran's Evolving Approach to Asymmetric Naval Warfare. The Washington Institute for Near East Policy

Hackers breach Iran rail network, disrupt service | Reuters. Reuters

APT35 Exploits Log4J Vulnerability to Distribute New Modular PowerShell Toolkit. Checkpoint

Iran Says Gas Stations Were Target Of Cyberattack To Foment Unrest (iranintl.com)

Complaint – Summons – Civil Cover Sheet.pdf (noticeofpleadings.com)