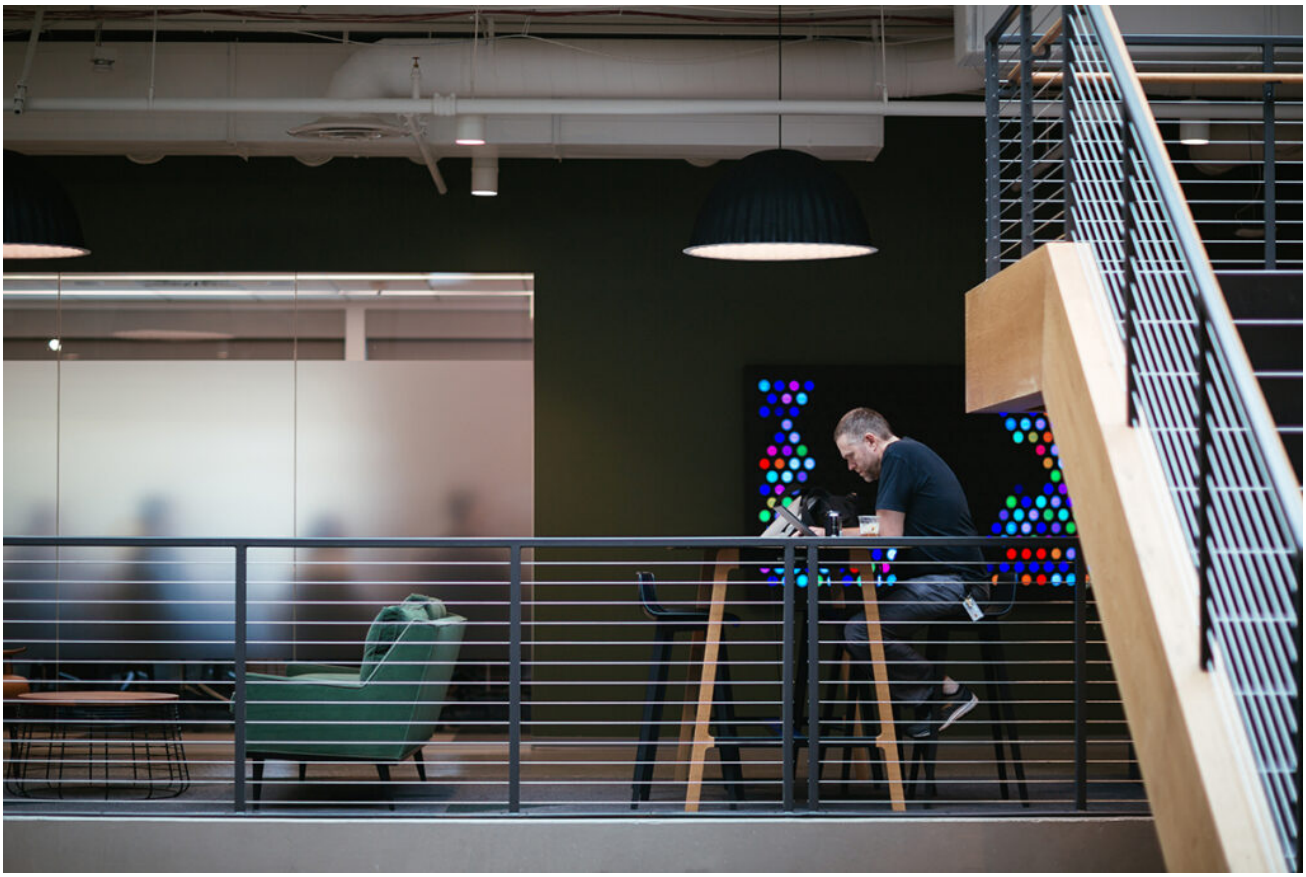
Malware distributor Storm-0324 facilitates ransomware access

microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/

September 12, 2023



By

The threat actor that Microsoft tracks as Storm-0324 is a financially motivated group known to gain initial access using email-based initial infection vectors and then hand off access to compromised networks to other threat actors. These handoffs frequently lead to ransomware deployment. Beginning in July 2023, Storm-0324 was observed distributing payloads using an open-source tool to send phishing lures through Microsoft Teams chats. This activity is not related to the Midnight Blizzard social engineering campaigns over Teams that we observed beginning in May 2023. Because Storm-0324 hands off access to other threat actors, identifying and remediating Storm-0324 activity can prevent more dangerous follow-on attacks like ransomware.

Storm-0324 (DEV-0324), which overlaps with threat groups tracked by other researchers as TA543 and Sagrid, acts as a distributor in the cybercriminal economy, providing a service to distribute the payloads of other attackers through phishing and exploit kit vectors. Storm-0324's tactics focus on highly evasive infection chains with payment and invoice lures. The actor is known to distribute the JSSLoader malware, which facilitates access for the ransomware-as-a-service (RaaS) actor Sangria Tempest (ELBRUS, Carbon Spider, FIN7). Previous distribution activity associated with Storm-0324 included the Gozi infostealer and the Nymaim downloader and locker.

In this blog, we provide a comprehensive analysis of Storm-0324 activity, covering their established tools, tactics, and procedures (TTPs) as observed in past campaigns as well as their more recent attacks. To defend against this threat actor, Microsoft customers can use Microsoft 365 Defender to detect Storm-0324 activity and significantly limit the impact of these attacks on networks. Additionally, by using the principle of least privilege, building credential hygiene, and following the other recommendations we provide in this blog, administrators can limit the destructive impact of ransomware even if the attackers can gain initial access.

Historical malware distribution activity

Storm-0324 manages a malware distribution chain and has used exploit kit and email-based vectors to deliver malware payloads. The actor's email chains are highly evasive, making use of traffic distribution systems (TDS) like BlackTDS and Keitaro, which provide identification and filtering capabilities to tailor user traffic. This filtering capability allows attackers to evade detection by certain IP ranges that might be security solutions, like malware sandboxes, while also successfully redirecting victims to their malicious download site.

Storm-0324's email themes typically reference invoices and payments, mimicking services such as DocuSign, Quickbooks, and others. Users are ultimately redirected to a SharePoint-hosted compressed file containing JavaScript that downloads the malicious DLL payload. Storm-0324 has used many file formats to launch the malicious JavaScript including Microsoft Office documents, Windows Script File (WSF), and VBScript, among others.

Storm-0324 has distributed a range of first-stage payloads since at least 2016, including:

- Nymaim, a first-stage downloader and locker
- Gozi version 3, an infostealer
- Trickbot, a modular malware platform
- Gootkit, a banking trojan
- Dridex, a banking trojan
- Sage ransomware
- GandCrab ransomware

- IcedID, a modular information-stealing malware

Since 2019, however, Storm-0324 has primarily distributed JSSLoader, handing off access to ransomware actor Sangria Tempest.

Ongoing Storm-0324 and Sangria Tempest JSSLoader email-based infection chain

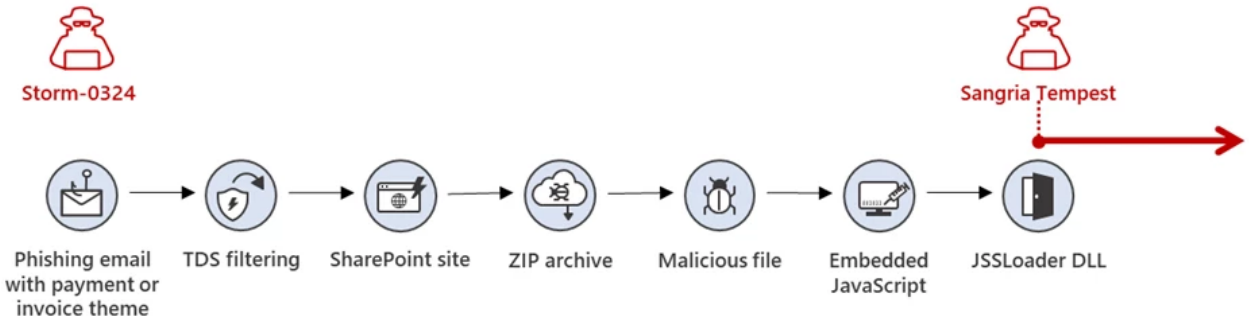


Figure 1. Storm-0324 JSSLoader infection chain based on mid-2023 activity

Since as early as 2019, Storm-0324 has handed off access to the cybercrime group Sangria Tempest after delivering the group's first-stage malware payload, JSSLoader. Storm-0324's delivery chain begins with phishing emails referencing invoices or payments and containing a link to a SharePoint site that hosts a ZIP archive. Microsoft continues to work across its platforms to identify abuse, take down malicious activity, and implement new proactive protections to discourage malicious actors from using our services.

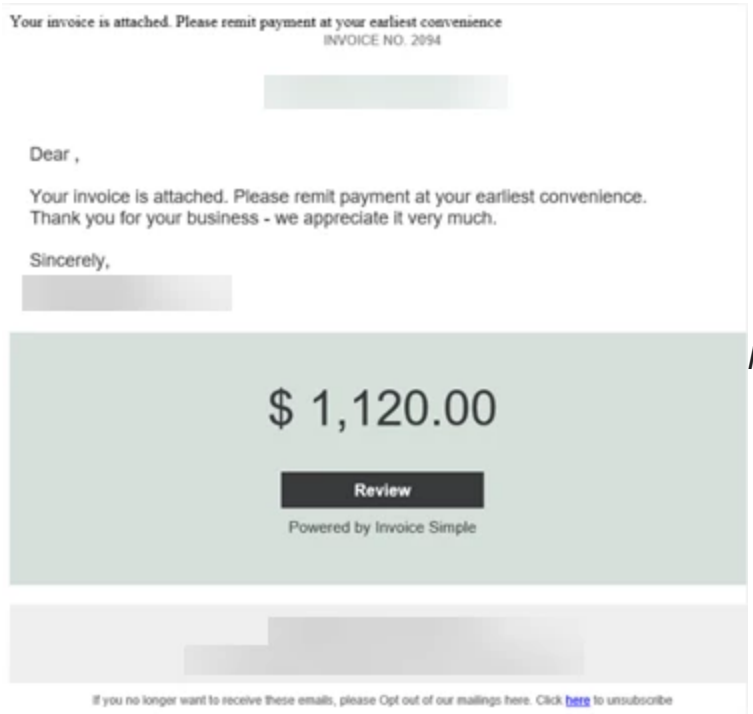


Figure 2. Example Storm-0324 email

The ZIP archive contains a file with embedded JavaScript code. Storm-0324 has used a variety of files to host the JavaScript code, including WSF and Ekipa publisher files exploiting the CVE-2023-21715 local security feature bypass vulnerability.

When the JavaScript launches, it drops a JSSLoader variant DLL. The JSSLoader malware is then followed by additional Sangria Tempest tooling.

In some cases, Storm-0324 uses protected documents for additional social engineering. By adding the security code or password in the initial communications to the user, the lure document may acquire an additional level of believability for the user. The password also serves as an effective anti-analysis measure because it requires user interaction after launch.

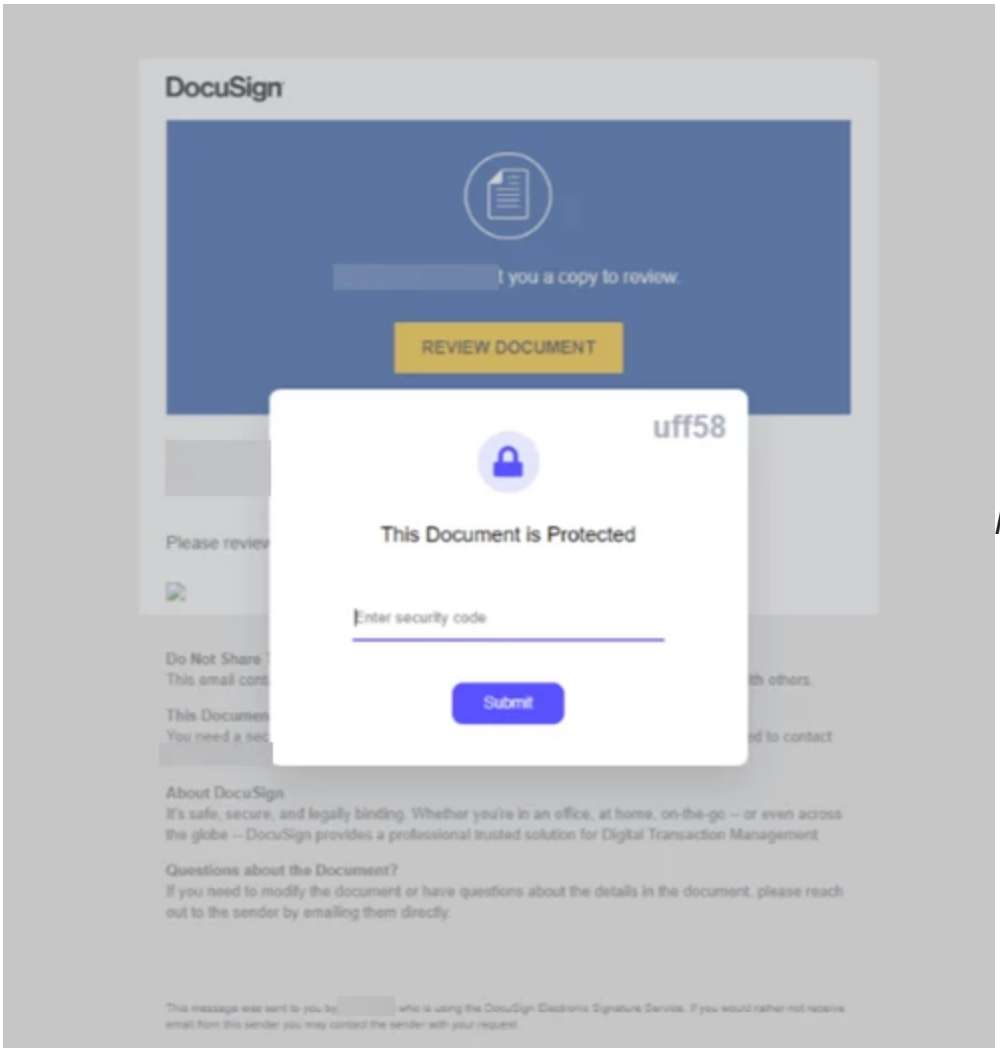


Figure 3. Storm-0324 password-protected lure document

New Teams-based phishing activity

In July 2023, Storm-0324 began using phishing lures sent over Teams with malicious links leading to a malicious SharePoint-hosted file. For this activity, Storm-0324 most likely relies on a publicly available tool called TeamsPhisher. TeamsPhisher is a Python-language program that enables Teams tenant users to attach files to messages sent to external tenants, which can be abused by attackers to deliver phishing attachments. These Teams-based phishing lures by threat actors are identified by the Teams platform as "EXTERNAL" users if external access is enabled in the organization.

Microsoft takes these phishing campaigns very seriously and has rolled out several improvements to better defend against these threats. In accordance with Microsoft policies, we have suspended identified accounts and tenants associated with inauthentic or fraudulent behavior. We have also rolled out enhancements to the Accept/Block experience in one-on-one chats within Teams, to emphasize the externality of a user and their email address so Teams users can better exercise caution by not interacting with unknown or malicious senders . We rolled out new restrictions on the creation of domains within tenants and improved notifications to tenant admins when new domains are created within their tenant. In addition to these specific enhancements, our development teams will continue to introduce additional preventative and detective measures to further protect customers from phishing attacks.

Recommendations

To harden networks against Storm-0324 attacks, defenders are advised to implement the following:

- Pilot and start deploying phishing-resistant authentication methods for users.
- Implement Conditional Access authentication strength to require phishing-resistant authentication for employees and external users for critical apps.
- Specify trusted Microsoft 365 organizations to define which external domains are allowed or blocked to chat and meet.
- Keep Microsoft 365 auditing enabled so that audit records could be investigated if required.
- Understand and select the best access settings for external collaboration for your organization.
- Allow only known devices that adhere to Microsoft's recommended security baselines.
- Educate users about social engineering and credential phishing attacks, including refraining from entering MFA codes sent via any form of unsolicited messages.
    - Educate Microsoft Teams users to verify 'External' tagging on communication attempts from external entities, be cautious about what they share, and never share their account information or authorize sign-in requests over chat.
- Educate users to review sign-in activity and mark suspicious sign-in attempts as "This wasn't me".

- Implement Conditional Access App Control in Microsoft Defender for Cloud Apps for users connecting from unmanaged devices.
- Configure Microsoft Defender for Office 365 to recheck links on click. Safe Links provides URL scanning and rewriting of inbound email messages in mail flow, and time-of-click verification of URLs and links in email messages, other Microsoft Office applications such as Teams, and other locations such as SharePoint Online. Safe Links scanning occurs in addition to the regular anti-spam and anti-malware protection in inbound email messages in Microsoft Exchange Online Protection (EOP). Safe Links scanning can help protect your organization from malicious links that are used in phishing and other attacks.
- Enable Zero-hour auto purge (ZAP) in Microsoft Office 365 to quarantine sent mail in response to newly acquired threat intelligence and retroactively neutralize malicious phishing, spam, or malware messages that have already been delivered to mailboxes.
- Practice the principle of least privilege and maintain credential hygiene. Avoid the use of domain-wide, administrator-level service accounts. Restricting local administrative privileges can help limit installation of RATs and other unwanted applications.
- Turn on cloud-delivered protection and automatic sample submission on Microsoft Defender Antivirus. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats.
- For additional recommendations on hardening your organization against ransomware attacks, refer to our threat overview on human-operated ransomware.

Microsoft customers can turn on attack surface reduction rules to prevent common attack techniques:

- Block executable files from running unless they meet a prevalence, age, or trusted list criterion
- Block JavaScript or VBScript from launching downloaded executable content
- Use advanced protection against ransomware

Detection details

Microsoft 365 Defender

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- TrojanSpy:MSIL/JSSLoader
- Trojan:Win32/Gootkit
- Trojan:Win32/IcedId
- Trojan:Win64/IcedId
- Trojan:Win32/Trickbot

Microsoft Defender for Endpoint

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

- Ransomware-linked Storm-0324 threat activity group detected

Hunting queries

Microsoft 365 Defender

Possible TeamsPhisher downloads The following query looks for downloaded files that were potentially facilitated by use of the TeamsPhisher tool. Defenders should customize the SharePoint domain name (‘mysharepointname’) in the query.

```
let allowedSharepointDomain = pack_array(
'mysharepointname' //customize Sharepoint domain name and add more domains as needed
for your query
);
//
let executable = pack_array(
'exe',
'dll',
'xll',
'msi',
'application'
);
let script = pack_array(
'ps1',
'py',
'vbs',
'bat'
);
let compressed = pack_array(
'rar',
'7z',
'zip',
'tar',
'gz'
);
//
let startTime = ago(1d);
let endTime = now();
DeviceFileEvents
| where Timestamp between (startTime..endTime)
| where ActionType =~ 'FileCreated'
| where InitiatingProcessFileName has 'teams.exe'
    or InitiatingProcessParentFileName has 'teams.exe'
| where InitiatingProcessFileName !has 'update.exe'
    and InitiatingProcessParentFileName !has 'update.exe'
| where FileOriginUrl has 'sharepoint'
    and FileOriginReferrerUrl has_any ('sharepoint', 'teams.microsoft')
| extend fileExt = tolower(tostring(split(FileName,'.')[-1]))
| where fileExt in (executable)
    or fileExt in (script)
    or fileExt in (compressed)
| extend fileGroup = iff( fileExt in (executable),'executable','')
| extend fileGroup = iff( fileExt in (script),'script',fileGroup)
| extend fileGroup = iff( fileExt in (compressed),'compressed',fileGroup)
//
| extend sharePoint_domain = tostring(split(FileOriginUrl,'/')[2])
| where not (sharePoint_domain has_any (allowedSharepointDomain))
| project-reorder Timestamp, DeviceId, DeviceName, sharePoint_domain, FileName,
FolderPath, SHA256, FileOriginUrl, FileOriginReferrerUrl
```

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. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy.

Microsoft Sentinel also has a range of detection and threat hunting content that customers can use to detect the post exploitation activity detailed in this blog in addition to Microsoft 365 Defender detections list above.

References

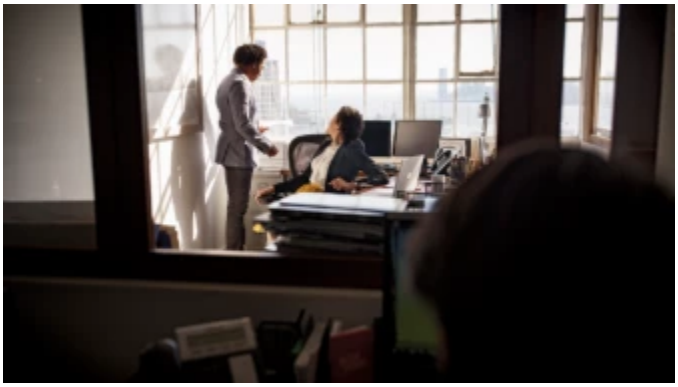
Further reading

Microsoft customers can refer to the report on this activity in Microsoft Defender Threat Intelligence and Microsoft 365 Defender for detections, assessment of impact, mitigation and recovery actions, and hunting guidance.

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on Twitter at https://twitter.com/MsftSecIntel.

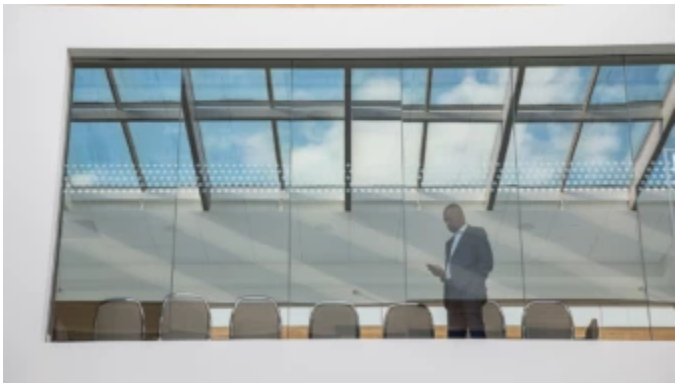
Related Posts



Research
Threat intelligence
Social engineering / phishing
Aug 26 min read

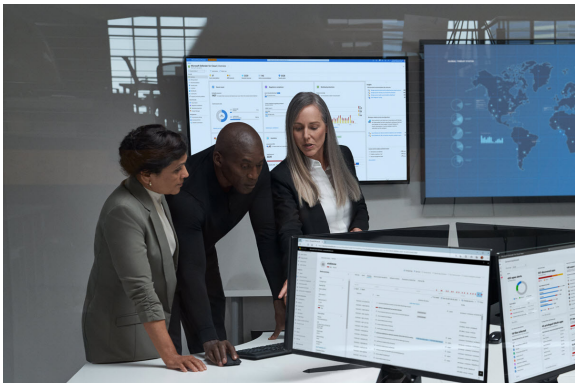
Midnight Blizzard conducts targeted social engineering over Microsoft Teams

Microsoft Threat Intelligence has identified highly targeted social engineering attacks using credential theft phishing lures sent as Microsoft Teams chats by the threat actor that Microsoft tracks as Midnight Blizzard (previously tracked as NOBELIUM).



Storm-0978 attacks reveal financial and espionage motives

Microsoft has identified a phishing campaign conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America. The campaign involved the abuse of CVE-2023-36884, which included a zero-day remote code execution vulnerability exploited via Microsoft Word documents.



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

Today, Microsoft is reporting on a distinct subset of Mint Sandstorm (formerly known as PHOSPHORUS), an Iranian threat actor that specializes in hacking into and stealing sensitive information from high-value targets. This subset is technically and operationally mature, capable of developing bespoke tooling and quickly weaponizing recently disclosed vulnerabilities.