Cyber Threat Actor "SingularityMD" Targeting K-12 Google Workspace Environments

November 2023 • SFAR-2023-6
TLP: GREEN

Note: This SFAR includes contributions from California IT in Education (CITE) and the California County Superintendents, Technology Services Committee (TSC).

Executive Summary

The MS-ISAC Cyber Threat Intelligence (CTI) team has recently observed the cyber threat actor (CTA) "SingularityMD" compromising K-12 student Google Workspace accounts for initial access. The CTA then leverages the compromised account and the environment's configurations to access and exfiltrate data to demand a ransom. The MS-ISAC CTI team assesses with moderate to high confidence that SingularityMD is likely to continue targeting K-12 organizations that use weak passwords and vulnerable configurations for Google Drive and Google Group. Please refer to the recommendations at the end of this report for further guidance.

Substantive Analysis

A trusted third party provided the MS-ISAC with an analysis of SingularityMD threat activity, showing that the CTA has been actively claiming access and threatening to leak sensitive public K-12 student data from at least four entities since October 2023.

In an interview with DataBreaches.net, SingularityMD explained their attacks, "We compromised a student account, then accessed information available to any student to escalate from there to teacher to systems level access for one or two systems. This was not a fancy high tech operation."[1] The CTA reportedly performs reconnaissance on social media and other public facing websites to collect personally identifiable information (PII) and email addresses for students. SingularityMD then uses that information to brute force weak student passwords that are based on PII, such as date of birth. A successive brute force compromise provides the CTA with initial access to K-12 school district Google Drive and Google Group accounts.

Once a student's account is compromised, the CTA leverages Google Workspace configurations to attempt to join Google Groups that allow access to material shared in Google Drives. The third-party analysis found that a school's Google Workspace configurations are sometimes set to allow a user to self-add themselves to another group by default. SingularityMD uses the compromised accounts to access and exfiltrate sensitive data including:

- Student and parent/guardian PII (first name, last name, student ID, home address, phone number, email address, race, and ethnicity)
- Student Photographs
- Data from Individualized Educational Programs (IEPs) and other Special Education (SPED) documents
- Person Summary Report (*see figure 1*)[2]
- Student incident reports
- Medical information

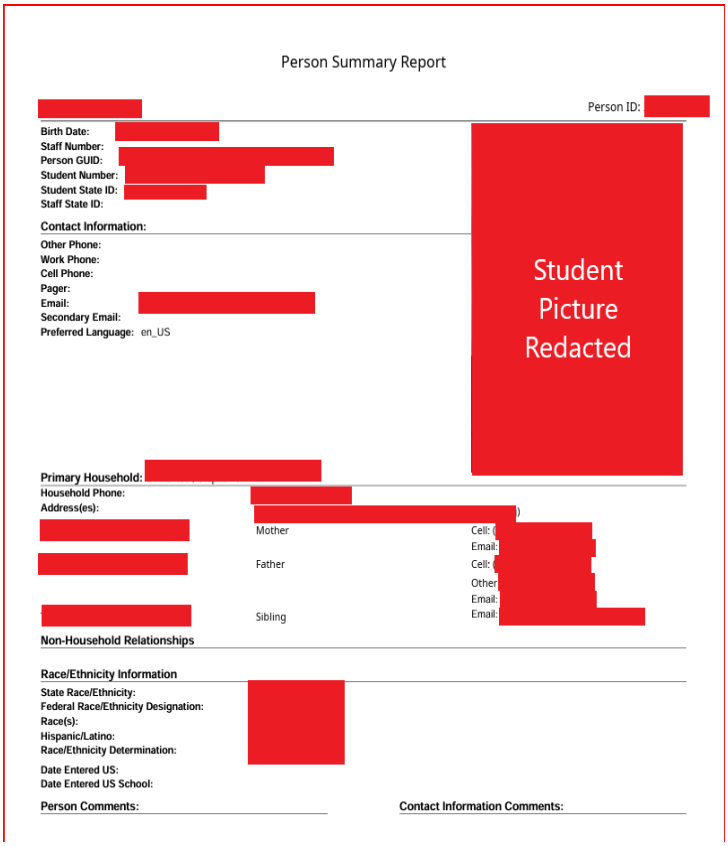

Figure 1: Example of a Summary Report containing Student PII. Source: DataBreaches.net

SingularityMD does not encrypt files during its intrusions. Instead, they exfiltrate sensitive victim data and request a ransom in exchange for destroying the stolen data.[3] School districts have reported that the CTA has emailed parents directly, threatening to leak the data to coerce school districts to meet the ransom demand. As with other CTAs, it is important to note that there is no guarantee that SingularityMD's will delete the stolen data if they receive a ransom payment.

SingularityMD's use of data exfiltration and extortion follows a trend the CTI team analyzed in SFAR 2023-04, highlighting ransomware groups' shift towards data extortion without encryption, enabling a growing contingent of CTAs to evade detection and increase the agility of their operations. In a recent post on BreachForums, SingularityMD expressed intentions to sell exfiltrated data as a service on the Dark Web which would offer an alternative revenue source from the ransom demands.

Notably, according to third party analysis, in several instances SingularityMD was able to use the compromised accounts to move from a Google cloud space to the local network system and exploit on-premise resources. Additionally, SingularityMD is known to use the compromised accounts to send phishing emails.

In a recent report, cybersecurity vendor Bitdefender highlighted similar threat activity where CTAs move laterally onto a local network and then abuse Google's Credential Provider for Windows (GCPW) to exfiltrate data from education institutions. According to the report, CTAs leverage the GCPW vulnerability to access "Google Classroom data, including classes, coursework, and student submissions, [that] could be exploited to manipulate educational data, impersonate students or teachers, or gain unauthorized access to educational resources."[4] The MS-ISAC CTI team cannot confirm whether SingularityMD was leveraging these tactics, techniques, and procedures (TTPs), but the parallels between their tactics and the malicious activity BitDefender described in their report are notable.

Indicators of Compromise

The below indicators of compromise (IOCs) are provided from California IT in Education (CITE) and California County Superintendents, Technology Services Committee (TSC). The IP addresses listed below **may not** represent active infrastructure but can be used for retroactive threat hunting.

IP addresses:

146.59.201[.]189

146.59.202[.]238

146.59.207[.]73

15.235.143[.]144

15.235.143[.]250

15.235.203[.]240

160.178.94[.]226

51.79.27[.]239

57.128.77[.]26

57.128.78[.]48

149.36.48[.]165

15.235.143[.]144

15.235.143[.]250

15.235.203[.]240

20.220.229[.]254

57.128.34[.]92

2a01:4f8:c012:5779[::]1

Email Addresses:

gmtst93@gmail[.]com

zezezuuuu@gmail[.]com

Analytic Confidence

Analytic confidence in this assessment is moderate to high. Source reliability is moderate to high with minimal conflict among sources. The lone exception is the BitDefender report, which highlights additional TTPs we cannot confirm SingularityMD engaged in. Time was three days to research this topic and the topic itself was not overly complex. The analysts worked amongst a small team to complete this product.

For questions or comments, please contact us at intel@cisecurity.org. For further information on our analytic tradecraft, please refer to our blog post outlining these standards.

Recommendations

The MS-ISAC will continue to monitor for similar activity and recommends the following actions:

Google Workspace Guidance and Configurations:

- Account managers and IT administrators should focus on their Google Workspace audits to check for malicious anomalies located within their user login audit logs.
- Additionally, administrators can use Security Command Center, a feature within Google, to set alerts for specific events related to SingularityMD's attack methods. Using this tool an administrator can create detailed policies to identify misconfigurations within accounts, group changes, misconfigurations in Identity and Access Management (IAM) roles, anomaly detection for data exfiltration, and password brute force attacks.

- Access control: Ensure users do not have the ability to add themselves to groups. This configuration setting should be changed to prevent user-initiated membership changes. IT administrators should audit of group memberships using native Google Admin tools, scripts, or products.
- Practice the principle of least privilege for shared resource permissions. This is particularly important for any shares storing personal or sensitive information using Google App Manager scripts or paid-for products that use Google Workspace Drive management software.
- Disable access to less secure apps for students through Google third-party app policy restrictions. Follow Google's recommendations for controlling access to less secure apps for further information.

Password Policy Management

- Implement multi-factor authentication where possible, such as for faculty and staff accounts.
- Use randomized, hard-to-guess passwords for student accounts.
    - Consider using "passphrases" instead of passwords — Length is the most important aspect of a good password.
- Consider offering password managers
    - System generated passwords created by a password manager are much stronger than human-created passwords. The password manager takes care of the storage and management of that password for the user.
- Instruct students and employees to avoid passwords tied to personal information. Avoid relying on information attackers can find about individuals on the internet. This can include date of birth, email address, or information from other public posts. For additional information regarding password policies refer to our CIS Password Policy Guide.

References

1. https://www.databreaches.net/hackers-escalate-leak-200k-ccsd-students-data-claim-to-still-have-access-to-ccsd-email-system/
2. https://www.databreaches.net/hackers-escalate-leak-200k-ccsd-students-data-claim-to-still-have-access-to-ccsd-email-system/
3. https://www.the74million.org/article/why-a-new-type-of-cyberattack-on-las-vegas-schools-should-worry-everyone/
4. https://www.bitdefender.com/blog/businessinsights/the-chain-reaction-new-methods-for-extending-local-breaches-in-google-workspace/

MS-ISAC®
EI-ISAC®

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722