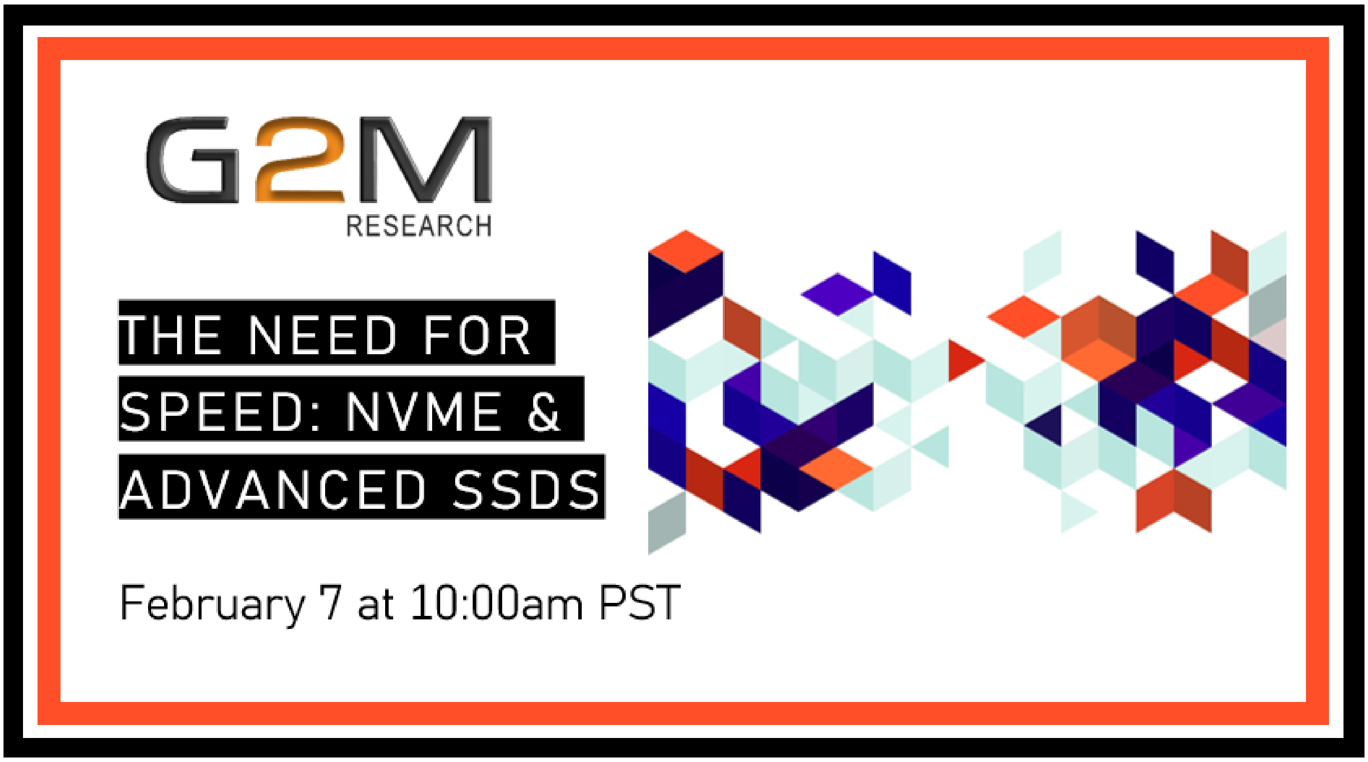
AI & Cybersecurity Newsletter

January 2023

Highlights

- Is Your Password “password”?
- Vice Society Targets Education Section & Switches From Using Existing Ransomware Tools To Their Own Signature Tool
- Free Cybersecurity Certifications & Courses
- 12M Daily Slack Users Sharing Proprietary Company Info, What Could Go Wrong?
- 2023 Webinar Schedule
- Upcoming Conferences



THE NEED FOR SPEED: NVME & ADVANCED SSDS

February 7 at 10:00am PST

Is Your Password “password”?

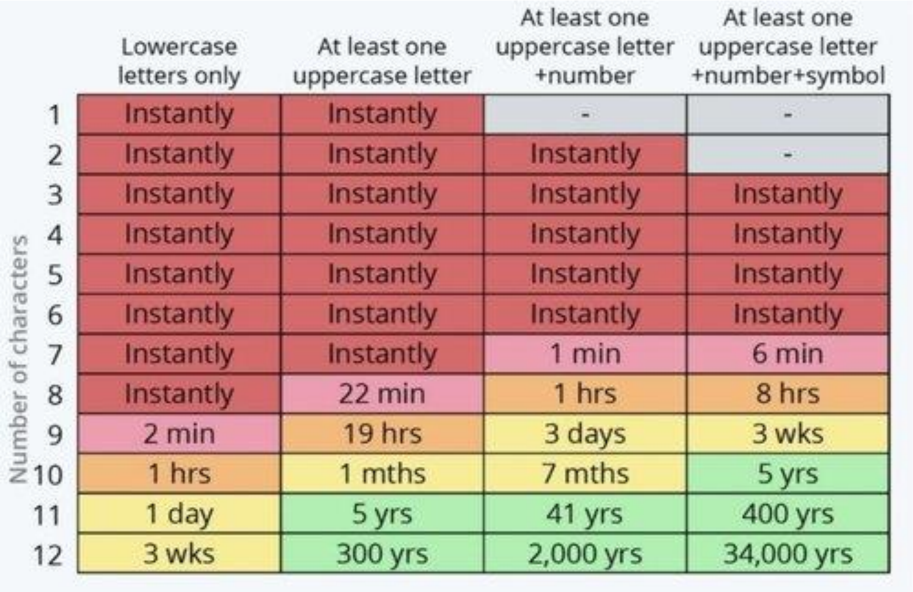
Posted by Karen Heumann, January 18, 2023

Criminals crack passwords using the following methods:

- Intercepting them as they are transmitted over the network.
- Brute force - automated guessing of millions of passwords.
- Physically stealing them, for example when they are written down close to a device.
- Searching IT infrastructure for stored password information.
- Manual guessing based on easily accessible personal information (e.g. name, date of birth).
- Shoulder surfing – observing people typing in their passwords in public places.
- Social engineering – tricking people into handing over passwords.
- Key-logging malware which records passwords as they are entered.

However, there isn’t a great need for sophistication or creativity given the top passwords of 2022 were:

1. password
2. 123456
3. 123456789
4. guest
5. qwerty
6. 12345678
7. 111111
8. 12345
9. col123456
10. 123123
11. 1234567
12. 1234



Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Nearly 5 million people around the world used “password” as their password. And, these common passwords were all guessed in under one second.

The Cybernews Investigation team collected data from publicly leaked data breaches to determine what passwords and phrases within passwords were used most. They analyzed **15,212,645,925 passwords**, of which 2,217,015,490 were unique and found:

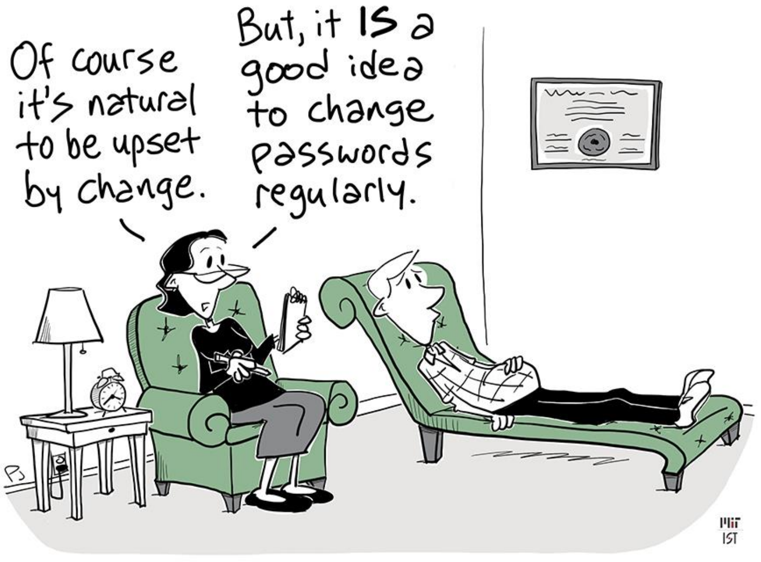
- When people use years as part of their password, they use their birth year, the year in which the password was created, or a special year (anniversary, child birthdate).
- The most commonly used name was Eva, followed by Alex, then Anna.
- Popular sports teams include the Phoenix Suns, Miami Heat, Cincinnati Reds, and Liverpool, Chelsea, and Arsenal soccer teams.
- Of 2.2 billion unique passwords, 7% included swear words.

Passwords that are easily cracked tend to include:

- Your actual or user name.
- Place names
- Family members' or pets' names / birthdays.
- Single dictionary words
- Personal information such as your date or place of birth.
- Favorite sports teams or other things relevant to your interests.
- Numerical or keyboard sequences (e.g. qwerty, 12345).

A key recommendation is to use a strong, non-predictable password that is at least 8 characters long and includes a combination of upper and lower case letters, symbols, and numbers. It is also important not to use the same password for everything. Websites have different levels of security. A criminal could hack a low security site and use that information to access important information on other sites.

On average, users use the same password across four different sites. Ideally, you should have a different password for every site and system you access. However, it can be difficult to remember that many passwords in practice. The main thing is to avoid using predictable passwords. Passwords should be easy to remember, but hard for somebody else to guess. The National Cyber Security Centre (NCSC) recommends that a good rule is to make sure that somebody who knows you well couldn't guess your password in 20 attempts.


Of course it's natural to be upset by change.
But, it IS a good idea to change passwords regularly.
MIT IST

Vice Society Targets Education Sector & Switches From Using Existing Ransomware Tools To Their Own Signature Tool

Posted by Mike Heumann, January 18, 2023

Vice Society ransomware group surfaced in June 2021, exploiting the PrintNightmare vulnerability (CVE-2021-1675 and CVE-2021-34527) to escalate privileges. They have been observed leveraging scheduled tasks, creating undocumented autostart Registry keys, and pointing legitimate services to their custom malicious dynamic link libraries (DLLs) through DLL side-loading. Vice Society actors attempt to evade detection through masquerading their malware and tools as legitimate files, using process injection, and likely use evasion techniques to defeat automated dynamic analysis. Vice Society actors escalate privileges, gain access to domain administrator accounts, and run scripts to change the passwords of victims' network accounts to prevent the victim from remediating.

Prior to deploying ransomware, the actors spend time exploring the network, identifying opportunities to increase accesses, and exfiltrate data for double extortion--a tactic whereby actors threaten to publicly release sensitive data unless a victim pays a ransom. Vice Society actors use tools ranging from SystemBC, PowerShell Empire, and Cobalt Strike to move laterally and “living off the land” techniques to target legitimate Windows Management Instrumentation (WMI) service and tainting shared content.

Historically, Vice Society ransomware group has attacked using Zeppelin, Five Hands, and HelloKitty ransomware. Now, they are executing attacks using a custom ransomware encrypt that implements a hybrid encryption scheme based on NTRUEncrypt and ChaCha20-Poly1305. SentinelOne discovered the new code and named it "PolyVice."

In September, a joint Cybersecurity Advisory (CSA) from the FBI, CISA and the MS-ISAC warned that Vice Society is disproportionately targeting the education sector with ransomware attacks. Other targeted sectors include healthcare and nongovernmental organizations (NGOs). Vice Society has infected organizations all over the world but mostly in the U.S. They are responsible for at least 100 attacks in the last 19 months, with 33 of the attacks on educational institutions.

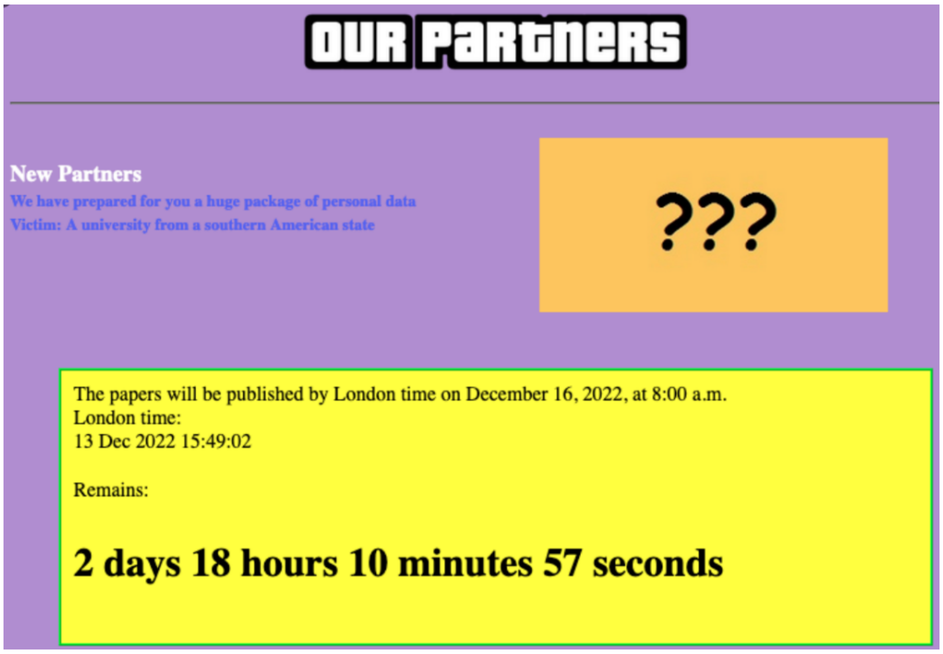
The education and healthcare sectors face many challenges in combating ransomware:

- A lack of budgeting for systems and security solutions has led many organizations to run legacy hardware that isn't patched against the latest vulnerabilities.
- Difficulties in controlling and managing personal devices brought in by students and staff. These personal devices introduce inherent risk because they interact with files via cloud services.
- The challenge of finding staff who trained to handle the ongoing threat of ransomware.
- These organizations are responsible for protecting vast amounts of highly sensitive and valuable personally identifiable information

PolyVice ransomware is a 64-bit binary that uses multi-threading for parallel symmetric data encryption, utilizing the victim's processor in full to speed up the encryption process. Each PolyVice worker reads the file content to determine what speed optimizations can be applied in each case. These optimizations depend on the file size, with PolyVice applying intermittent encryption selectively. After encryption, each PolyVice worker writes the file footer with information necessary for decryption.

Vice Society attacked the Los Angeles Unified School District in the first week of September and crippled digital operations across the system, which includes more than 1,000 schools and serves roughly 600,000 students. Two weeks after the initial attack, as the district worked to recover and restore its systems, the hackers said that they would leak the 500 gigabytes of data they claimed to have stolen from LAUSD if the school system didn't pay a ransom. The district refused to pay and the hackers released student data including Social Security numbers, tax information, and health data.

"We would probably think of them as a second- or maybe third-tier group overall, compared to big names like LockBit, Hive, and Black Cat," says Allan Liska, Recorded Future Solutions Architect. "But the bulk of their victims are either in the education or health care sectors, and their attacks make up a significant chunk of the total known attacks in those categories for 2021 and 2022." "They're a perfect example of the success of mediocrity in the ransomware ecosystem," says Claire Tills, Senior Research Engineer, Tenable. "You have the top-tier groups developing their own zero days and acting all polished and professional. But meanwhile, Vice Society is just chugging along, not really innovating, stealing tools from other folks, but they have just enough stability to launch attacks, get paid, keep moving."



OUR PARTNERS

New Partners
We have prepared for you a huge package of personal data
Victim: A university from a southern American state

???

The papers will be published by London time on December 16, 2022, at 8:00 a.m.
London time:
13 Dec 2022 15:49:02

Remains:

2 days 18 hours 10 minutes 57 seconds

Free Cybersecurity Certifications & Courses

Posted by Mike Heumann, January 18, 2023

7 Free Cybersecurity Certifications from CISA (Cyber & Infrastructure Security Agency):

Cyber Essentials - Managing cyber risks requires building a culture of cyber readiness. This training will cover what it means to be cyber-ready and how to enable a cyber-ready culture in your organization.

Cloud Security - video

Cloud Computing Security – pdf and video

Cyber Supply Chain Risk Management for the Public

Fundamentals of Cyber Risk Management

Introduction to Cyber Intelligence

Securing Internet Accessible Systems

Free Cybersecurity Certifications:

Skillfront ISO27001 Information Security Associate

Cisco Cloud Security Certification

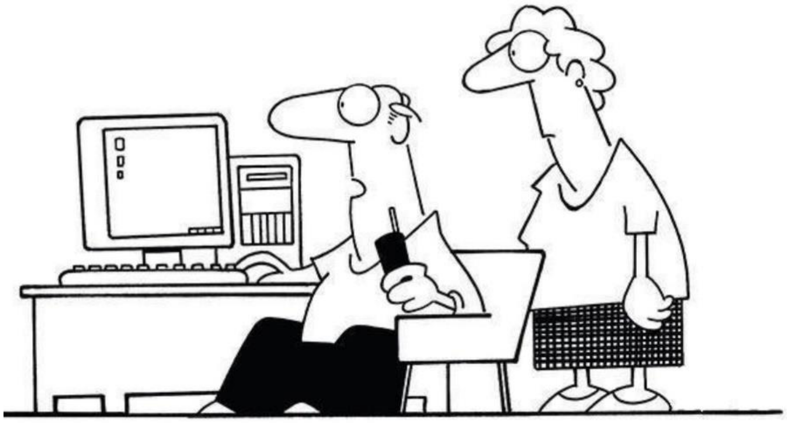
Cisco Certified Network Associate Certification

Fortigate Security Certification

Fortigate EDR Certification

KALI Linux Fundamentals

Certified Information Security Manager



“Tech support says the problem is located somewhere between the keyboard and my chair.”

Free Cybersecurity Classes

Cybersecurity for Everyone by the University of Maryland

Cloud Security Basics by the University of Minnesota

Introduction to Cybersecurity by the University of Washington

Introduction to Cyber Security by the Open University

Internet History, Technology, and Security by the University of Michigan

12M Daily Slack Users Sharing Proprietary Company Info, What Could Go Wrong?

Posted by Karen Heumann, January 18, 2023

Slack is used by 100k+ organizations, including 77 of the Fortune 100 companies. Slack breaks down silos and creates an open forum for troubleshooting, sharing ideas, finding common interests, and venting. But, 12M+ daily users (and, a jaw-dropping 79M+ users expected by 2025) and rapid-fire exchange, across multiple channels, with people you have never met before, creates a cybersecurity risk rich environment. The benefit of Slack? Users relax and collaborate freely. The risk? Users don't consider the hacking risks and may not question whether the person asking for confidential data is the authorized recipient of that information or may click on a shared article without the poster or viewer recognizing the document is infected. Obviously, it is not the fault of the platform if someone mistakenly or maliciously shares an infected document, but the risks should be recognized and minimized. Just as employees are trained to recognize phishing emails, consideration should be given to the risks inherent in Slack, and other communication platforms.

End-to-end encryption is becoming a standard means to secure digital conversations, authorizing only the sender and the recipient to view the messages and all the data contained within. However, Slack does not have end-to-end encryption in order to retain visibility into communications across working groups and slack channels. Slack does use HTTPS encryption, DLP integrations, and its own Enterprise Key Management (EKM) for data protection. This means data is encrypted both enroute and while at rest on Slack's servers. If a hacker obtained the decryption key, they could access all the messages sent across the platform, including confidential data, and more importantly, the thought processes behind developing, resolving, and addressing product development, revenue strengths and weaknesses, planned projects, sales metrics, personnel grievances, and company strategy. The huge volume of message-creation on Slack provides an especially large attack surface.

Slack was hacked in December. The security team found that some Slack employee tokens were stolen and used to access the company's GitHub external repository. No downloaded repositories contained customer data. Also, last July an independent security researcher discovered a vulnerability when the platform transmitted a hashed version of the user password to other workspace members. This hashed password was not visible to any Slack clients and discovering it required actively monitoring encrypted network traffic coming from Slack's servers. The flaw affected all users who created or revoked shared invitation links between April 2017 and July 2022.

BetterCloud's Christina Wang is concerned that Slack users with "Owner" and "Admin" roles have significant power, often more than most administrators realize. For example, Wang says, "By default, only Slack Workspace Admins and Owners can create and manage user groups. But any admin can change those settings in a drop-down menu." Effectively, any one of your organization's admins can go in and make it possible for all of a workspace's users to create, modify or disable user groups.

Ars Technica reported that "A surprisingly large number of developers are posting their Slack login credentials to GitHub and other public websites." Despite Slack declaring that access tokens should be treated with the same level of care as passwords. The Origin Report's Josh Fraser shared that the 1,118 members of its open Slack community had their personal information — including their email addresses, usernames, real names, profile pictures, last updated timestamps and timezone settings — exposed by a hacker who manipulated API keys.

Also, very little is known about which Slack team members can access user data, and when they can do it. Slack claims to have technical, audit and policy controls in place to prevent inappropriate access, they also acknowledge that they did not intentionally build an app that would prevent employees from accessing information without authorization. Electronic Frontiers Foundation Senior Staff Attorney Nate Cardozo says, "Slack could have built this system in a way that no one within the company had access into user data," referencing zero-knowledge encryption, an end-to-end encryption method. "What it comes down to is, trust us.'"

G2M Research Multi-Vendor Webinar Series

Our webinar schedule is below. Registration links and more information will be available in our next newsletter, on our website, and you can always contact us directly with questions. We are offering a Cybersecurity series and an Enterprise Storage & Technology multivendor series.

January 12, three cybersecurity industry leaders joined us for a discussion about “Bug Bounties Gone Bad? Uber Case Highlights Pressure on CISOs.” Matt Johnson, Principal Security Architect at IBM, Tony Anscombe, Chief Security Evangelist at ESET, and Garret Grajek, CES, CISSP, Chief Executive Officer at YouAttest provided thoughtful insight into the issues around bug bounties, ransomware, and, particularly, best practices in communicating and resolving organizational breaches. The webinar video is available to view and a copy of the slidedeck is available here.

Interested in Sponsoring a webinar? Contact G2M for a prospectus. We can create custom webinar, custom webinar series, and add or modify topics to specifically appeal to your target audience. View our webinars and access slide deck presentations on our website.

Cybersecurity

Cybersecurity for Remote Workers & Mobile Devices	March 23
The Increasing Complexity of Cybersecurity Regulatory & Compliance for the Financial Services Industry	May 25
xDR- The Promise versus the Reality	August 3
10 Features of an Effective Attack Surface Management Tool	September 7
How Secure is the Cloud for Your Workloads?	October 12
Do You Need a SIEM? Use Cases Where a SIEM Makes Sense.	November 9

Enterprise Storage & Technology

The Need for Speed: NMVe & Advanced SSDs	February 7
Memory As The New Storage – CXL, Extended Memory, & Persistent Memory. What Does the Future Hold?	March 7
Storage Architectures for Artificial Intelligence & Machine Learning	April 4
Software-Defined Flash Memory Architectures	May 9
Storage & Compute Architectures for Healthcare & Imaging Applications	June 27
NVMe & NVMe-oF – Past, Present, & Future	July 11
GPUs, SSDs, & Shared Memory: Accelerating Computing?	August 22
Securing Data – How Storage & Cybersecurity Technologies Can Work Together	Sept 26
The Open Compute Platform (OCP) Movement – Providing Compute-At-Scale Value to On-Premises Deployments	October 24
Storage Architectures for HPC Clusters	November 21
2024 Trends – Cloud, On-Premises, & Hybrid Compute/Storage	December 12

Upcoming Conferences

January 18	SNIA Persistent Memory Summit, San Jose, CA
January 30-Feb 1	Cybertech Global TLV, Tel Aviv, Israel
February 6-10	Cisco Live, Amsterdam, Netherlands
February 13-14	Gartner Security & Risk Management, Mumbai, India
February 14-16	ESNA Expo, Long Beach, CA
February 14-17	ITExpo East, Fort Lauderdale, FL
February 27-28	Gartner Security & Risk Management Summit, Dubai
February 27-March 2	Mobile World Congress Barcelona
February 28-March 2	Rice University Energy HPCC Conference, Houston, TX
March 8-9	CloudExpo Europe, London
March 14-16	Gulf Information Security Expo, Dubai, UAE
March 20-22	Gartner Data & Analytics Summit, Grapevine, TX
March 20-23	GTC CPU Technology Conference, San Jose, CA
March 28-29	Gartner Security & Risk Management, Sydney, Australia
March 28-31	ISC West, Las Vegas
April 5-7	IST Information Security Expo, Tokyo, Japan
April 15-19	NABShow, Las Vegas
April 17-21	HIMMS Global Health Conference, Chicago, IL
April 17-21	Privacy Symposium, Venice, Italy
April 19-20	CyberSec Europe, Brussels, Belgium
April 24-27	RSA Conference, San Francisco

May 1-3	IAHSS AC&E, Nashville, TN
May 2-4	ACT Expo, Anaheim, CA
May 9-12	Black Hat Asia 2023, Singapore
May 15-17	Forth Roadmap Conference, Portland, OR
May 16-17	SIA GovSummit, Washington DC
May 21-25	ISC, Frankfurt, Germany
May 22-25	Dell World, Las Vegas
May 22-25	Government Fleet Expo, Dallas, TX
June 2-6	School Transportation Network Expo East, Indianapolis, IN
June 4-8	Cisco Live, Las Vegas
June 5-7	Gartner Security & Risk Managemnt, National Harbor, MD
June 7-9	Synnex Red, White and You, Greenville, SC
June 11-14	36th Electric Vehicle Symposium & Expo, Sacramento, CA
June 14-16	Interop Tokyo, Chiba, Japan
June 20-22	HPE Discover, Las Vegas
June 20-22	Info Security Europe, London
July 14-19	School Transportation Network Expo, Reno, NV
August 5-10	Black Hat USA, Las Vegas
August 8-10	Flash Memory Summit, Santa Clara, CA
August 28-31	VMWare Explore, US, San Francisco, CA
August 30-Sept 1	Security Expo, Sydney, Australia
September 11-13	Gartner Security & Risk Management, London
September 11-13	Global Security Exchange, Dallas, TX

G2M RESEARCH

Effective Marketing & Communications
with Quantifiable Results