G2M RESEARCH

AI & Cybersecurity Newsletter

MAY 2021

Highlights

RSA Conference 2021: COVID & the Expanded Attack Surface

Non-Fungible Tokens – Useful or Irrelevant?

SolarWinds: What Really Happened?

Colonial Pipeline Attack & Why You Should Not Hoard Gas in Plastic Tubs

Poll Results, Webinar Schedule, Upcoming AI & Cybersecurity Events

Our multivendor webinars allow engagement, whether from competing perspectives or compatible approaches, at a substantive level, and allows for hundreds of attendees to have the same front row seat. The conversations feel spontaneous, there is a rapport and dialogue that can go deep with each panelist having a solid opportunity to argue their perspective. Plus, the high-quality recorded webinar and slide deck remain available for use long after the event.

We have a cybersecurity deep dive on Tuesday, May 25th at 10:00am PST with “How to Take a 360 Degree View of Cybersecurity.” Cybersecurity is, or should be, a major concern for any organization today. The need to protect your data, protect your customers/clients, and cost savings of avoiding a breach, and the value of maintaining your business reputation and industry confidence are just a few obvious reasons to invest time, money, and effort in all aspects of cybersecurity.

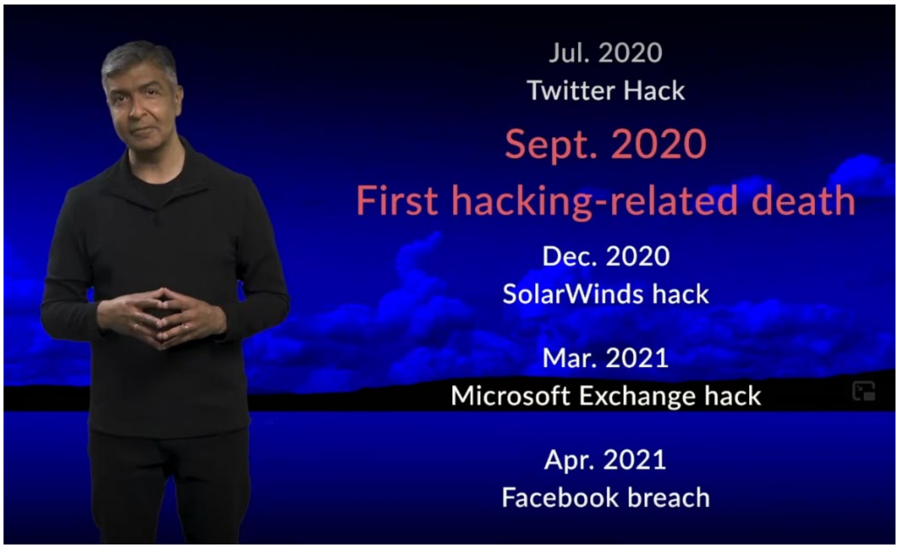
If you are interested in sponsoring a webinar but don’t see a topic that quite fits your needs, we can modify topics or add topics to meet your objectives. Our entire webinar schedule, poll results from a prior webinar, and other upcoming AI and Cybersecurity events are at the end of our newsletter.

Cheers! Mike Heumann

"How to take a
360 Degree View of Cybersecurity"
Tuesday, May 25 at 10:00am PST
SecurityScorecard
Crowe
G2M
RESEARCH

RSA Conference 2021
COVID & the Expanded Attack Surface

RSAC Virtual 2021 kicked off on Monday May 17th with a keynote titled "A Resilient Journey" from Rohit Ghai, RSA's CEO. Unsurprisingly, one of the big themes of the keynote was how COVID-19 forced IT and IT security to rethink how we approach remote workers, trust, resiliency, and hacks when most of the workforce of a variety of companies were forced to work remotely. BYOD (bring your own device) went from being an interesting (and sometimes painful) use case to one that was the overwhelmingly common use case for employees. We also went from in-person meetings to "Zoom everywhere".



Jul. 2020
Twitter Hack

Sept. 2020
First hacking-related death

Dec. 2020
SolarWinds hack

Mar. 2021
Microsoft Exchange hack

Apr. 2021
Facebook breach

These changes radically expanded the attack surface that cybercriminals and malicious state actors could (and did) try to exploit in 2020-2021, with results including the SolarWinds Hack (Dec 2020), the Colonial Pipeline hack (May 2021), Microsoft Exchange hacks (March 2021), and a variety of other attacks. Rohit also stated that there is an equal number of attacks that were prevented or mitigated, including the FBI's "cleaning" of Exchange Servers in April, the US elections (largely without issue), and the stopping in February 2020 of the largest DDOS attack to date.

What we have learned to date in these new times:

- "Zero Trust" and "100% authentication" is morphing into continuous authentication – looking not only at credentials, but user activity and behavior throughout their presence on IT resources, and not just at login.
- Sharing information across organizations is critical to identifying issues (essentially how the SolarWinds hack was exposed).
- Third-party/fourth-party risk management is a real issue, as illustrated by the SolarWinds hack, which showed how supply chains and vendors to our vendors can be exploited by hackers.

Non-Fungible Tokens – Useful or Irrelevant?

Two questions addressed at RSAC regarding the utility of non-fungible tokens (NFTs) asked:

- Are they relevant? And,
- Why are they a subject of discussion for RSA?

For those of you who are not familiar with NFTs, they are a "marker" that can be associated with digital assets such as pictures, artwork, movies, books, or even more complex types of digital data. NFTs can be tracked through blockchains to provide proof of ownership of an asset. Believe it or not, the NFT market is worth $250 million, 3x more than in 2020.

While many of the experts on the RSAC panel generally questioned the value of NFTs, the use case for them seems fairly clear – proving the provenance and ownership of digital assets. Their second question – "Why are we talking about NFTs at RSAC?" was more interesting (if not necessarily pertinent). While RSAC (and the company RSA) started around cryptography, RSAC has morphed into the premiere cybersecurity show on the planet today. NFTs are low on the list of concerns for most enterprise CISO organizations. And, as Jack Morse, interpreted the panel to indicate, nonfungible tokens are basically, "dumb as hell."

Panelist Ron Rivest, a famed cryptographer who co-created RSA public-key encryption, derided non-fungible tokens as worth even less than the famed tulips of tulip mania.

At least with actual tulips, argued Rivest, "you can own them, you can possess them, you can plant them, you can enjoy them."

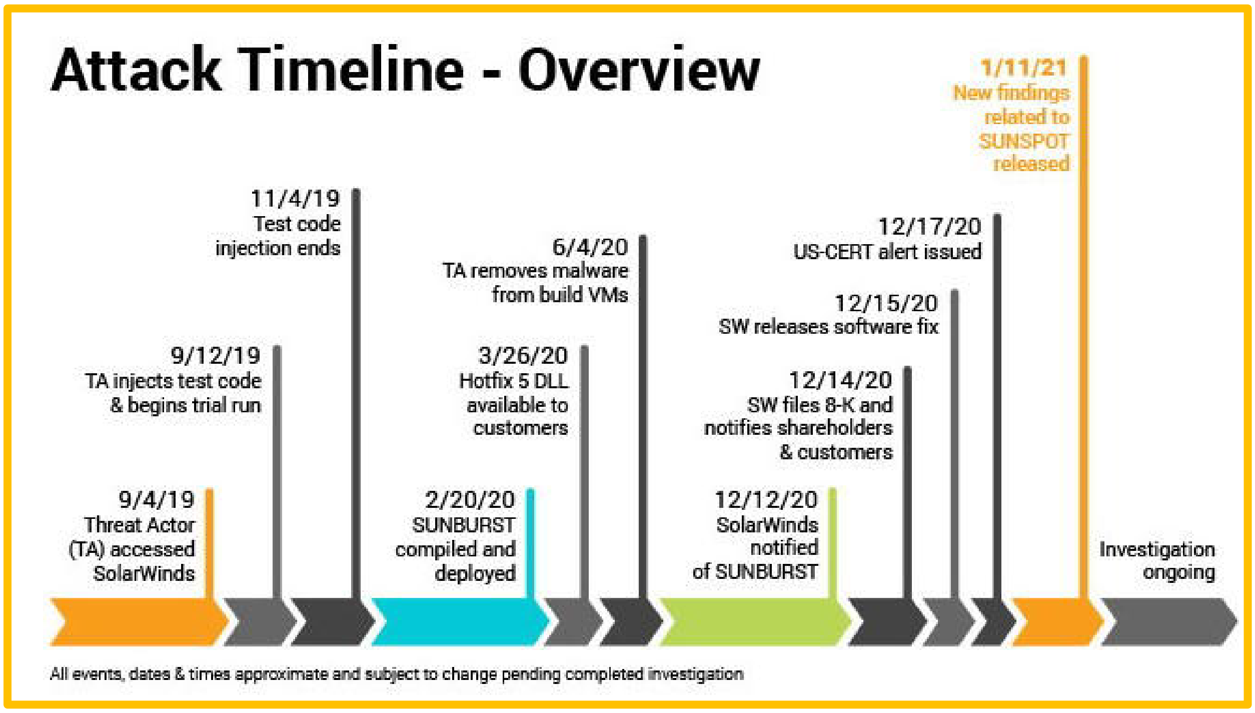
NFTs, Rivest observed, aren't even like pictures of tulips. They're more akin to digital tokens that point at a picture of a tulip.

"It's a bit like homeopathic medicine," said Rivest. "You dilute it, you dilute it, you dilute it, and you say, 'What's left?'"

Professor Ronald Rivest is an Institute Professor at MIT, member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and a founder of its Cryptography and Information Security Group.

SolarWinds: What Really Happened?
RSA Conference 2021

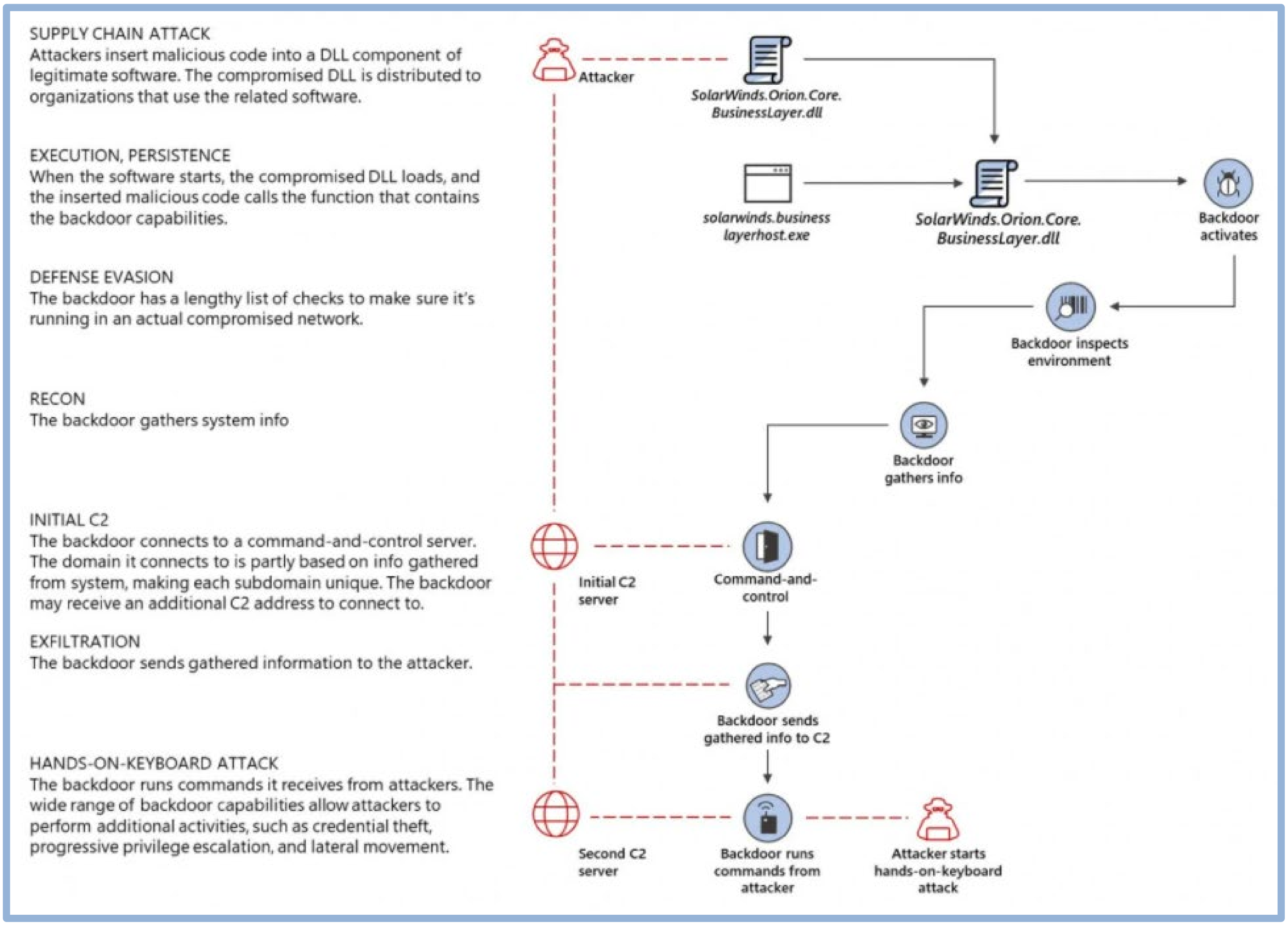
Sudhakar Ramakrishna, now President and CEO of SolarWinds, brings 25 years of experience to his new role, including as CEO of Pulse Secure. Laura Koetzle, Security Risk Analyst for Forrester's European, interviewed Ramakrishna regarding the SolarWinds breach and aftermath as part of RSA Conference 2021. Ramakrishna became CEO of SolarWinds a month after



Attack Timeline - Overview
9/4/19 Threat Actor (TA) accessed SolarWinds
9/12/19 TA injects test code & begins trial run
11/4/19 Test code injection ends
2/20/20 SUNBURST compiled and deployed
3/26/20 Hotfix 5 DLL available to customers
6/4/20 TA removes malware from build VMs
12/12/20 SolarWinds notified of SUNBURST
12/14/20 SW files 8-K and notifies shareholders & customers
12/15/20 SW releases software fix
12/17/20 US-CERT alert issued
1/11/21 New findings related to SUNSPOT released
Investigation ongoing

All events, dates & times approximate and subject to change pending completed investigation news of the breach. The breach went undetected for months and US agencies — including parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury — were attacked.

Ramakrishna has a positive, focused perspective on the circumstances, highlighting, “The important thing to recognize for all of us, no matter how big or small we are, is that we all have to be prepared at all points in time, to be humble enough to accept that security vulnerabilities and breaches can happen to anyone, notwithstanding what resources we have and how good and great we are. So, one thing that my Pulse Secure experience taught me, and even in prior companies, I would say, is that at all points, you have to be vigilant, but all points you have to be humble because you cannot think this won’t happen to you, it might only happen to others. So, when you have that mindset of always being vigilant, always being humble, transparency is very, very important, because it’s critical to know what’s happening. And, when something happens, that you are able to communicate it, project it, take ownership and do something about it.”



SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it’s running in an actual compromised network.

RECON
The backdoor gathers system info

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION
The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.

Attacker
SolarWinds.Orion.Core.BusinessLayer.dll
solarwinds.businesslayerhost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Backdoor activates
Backdoor inspects environment
Backdoor gathers info
Initial C2 server
Command-and-control
Backdoor sends gathered info to C2
Second C2 server
Backdoor runs commands from attacker
Attacker starts hands-on-keyboard attack

Colonial Pipeline Attack & Why You Should Not Hoard Gas in Plastic Tubs

A ransomware attack on Colonial Pipeline by hacking group DarkSide crippled gas and jet fuel supplies to nearly half the east coast. The pipeline is 5,500 miles long and can carry 3M barrels of fuel each day. The pipeline is owned by the Koch Industries (28%), South Korea’s National Pension Service and Keats Pipeline Investors LP (23.44%), CDPQ Colonial Partners, LP (16.55%), Shell Pipeline Company, LP (16.55%), and IFM Colonial Pipeline (15.8%).

Colonial Pipeline paid $4.4M in ransomware to prevent a longer shutdown of services. DarkSide announced that their servers had been seized and their cryptocurrency drained. Joseph Blunt, Colonial Pipeline President and CEO will testify to the House Homeland Security Congressional Committee regarding the cyberattack on June 9.

Last year, Colonial Pipeline gasoline pipeline leaked 1.2M gallons of gas into a nature preserve in North Carolina which went undetected for weeks until a group of teenagers passing through the area noticed liquid gurgling and spreading downhill. It took five days to repair a five-foot crack in the pipeline and five months to recover 800k gallons of gasoline. In 1996 Colonial spilled 1M gallons of fuel in South Carolina, pleaded guilty to criminal negligence and was fined $41M under the Clean Water Act.

Both parties regret all the attention this breach as created. Blount stated, “We were perfectly happy having no one know who Colonial Pipeline was, and unfortunately that's not the case anymore," he said. "Everybody in the world knows."

At the time of the hack, the DarkSide criminal gang acknowledged the incident in a public statement. "Our goal is to make money and not creating problems for society," DarkSide wrote on its website. "We do not participate in geopolitics, do not need to tie us with a defined government and look for... our motives," the group added.

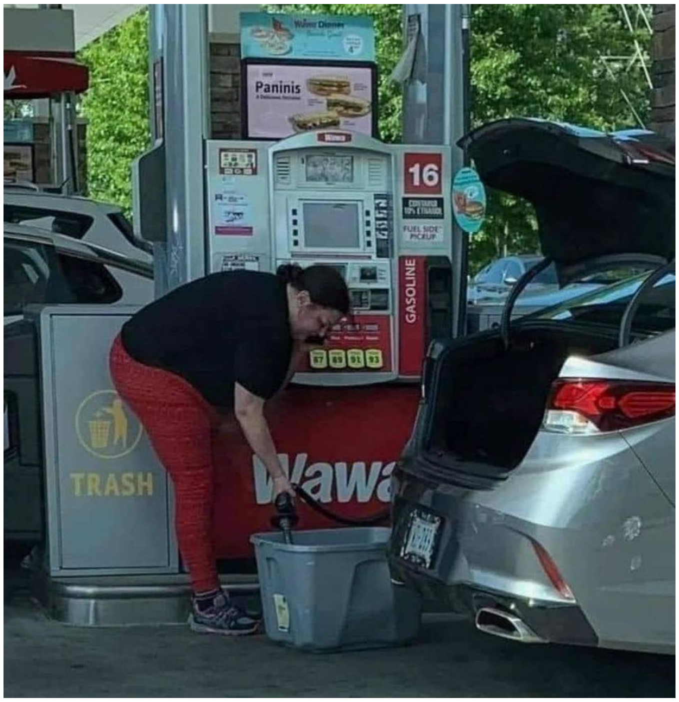
The ransomware attack is the second known such incident aimed at a pipeline operator. Last year, the Cybersecurity and Infrastructure Security Agency reported a ransomware attack on a natural gas compression facility belonging to a pipeline operator. That caused a shutdown of the facility for two days, though the agency never revealed the company's name.

Meantime…. As gas shortages loomed and commuters lined up for hours to tap dwindling gas supplies, some artful motorists attempted to stash a bit of extra gasoline… Leading us to share…

Why you should not hoard gasoline in plastic tubs:

1) Gasoline expires. It does not have an indefinite shelf life.
2) Gasoline eats through many plastics causing gas spills, unhealthy vapors, fire risk, general mess, and smell.
3) Even if the gasoline does not completely eat through the plastic, residue from the plastic can cause damage to the car engine.
4) Tubs full of gas are heavy. How will she lift it into the car?
5) Liquids slosh. Is there a lid somewhere? (a very tight lid?)
6) By the way, is she talking on her cell phone? Maybe planning to smoke a cigarette on the drive home? Gasoline is flammable.
7) If she is in a car accident or has to stop suddenly, um…
8) And….Okay, she fills the tub, lifts it with no problem, does not have to stop suddenly, gets it home, and it does not expire….

   How does she get the gas from the plastic tub into the tank?



Utilizing HPC-Scale Storage and AI for Business Intelligence

with sponsors Samsung, WekaIO, Datyra, NVIDIA

Has your organization explored and/or deployed AI-based systems for business intelligence yet? (check one):

We **have deployed AI for a variety** of business applications:	38%
We **have deployed AI for a couple** of business applications:	15%
We are performing proof of concept evaluations on AI solutions, **with the idea of deploying them in the near future**:	31%
We are **talking to vendors about potential AI solutions**:	0%
We **are not actively exploring using AI** in our organization:	15%

Utilizing HPC-Scale Storage and AI for Business Intelligence

What do you see as the greatest challenge for your organization to implement an AI solution? (check all that apply):

Understanding what business value we can reasonably expect from AI:	27%
Finding the **right vendor** and/or people to implement an AI solution:	20%
Building the right training data set:	40%
Affording the hardware required for a meaningful AI solution:	13%
Achieving the right level hardware and software **performance**:	40%
Other issues:	7%

G2M Research Multi-Vendor Webinar Series

Our webinar calendar - including an enterprise storage and cybersecurity webinar this month.

You can view our webinars and access the full slide deck presentations.

G2M RESEARCH

May 25:	How to Take a 360 Degree View of Your Organization's Cybersecurity
June 15:	It's 2021 - Where Has NVMe-oF™ Progressed To?
July 13:	Computational Storage vs Virtualized Computation/Storage in the Datacenter: "And The Winner Is"?
Aug 17:	AI/ML Storage - Distributed vs Centralized Architectures
Sept 14:	Composable Infrastructure vs Hyper-Converged Infrastructure for Business Intelligence
Oct 12:	Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
Nov 9:	The Radiometry Data Explosion: Can Storage Keep Pace?
Dec 14:	2021 Enterprise Storage Wrap-up Panel Discussion

AI & Cybersecurity Events – All Virtual

May 22-23	The Role of AI in Cybersecurity
May 26	Cyber Trends 2021
May 26	Securing the Supply Chain of Critical Technologies, Products, & Systems
May 27	The Usual Misperception of Business Leaders to Cybersecurity
May 27	Cybersecurity Culture
June 1	Cybersecurity in iGaming: Secure by Design
June 15	The Global Dilemma. Meeting the AI, Cybersecurity, & Cloud Challenges
June 15	The Future of Cybersecurity in a Post-Covid World
June 22	Think Cybersecurity for Government 2021
July 14	The Future of AI
July 16-17	The Diana Initiative

G2M COMMUNICATIONS

Effective Marketing & Communications with Quantifiable Results