AI & Cybersecurity Newsletter
September 2020

Highlights:
[Ransomware Attack Intended for University Hits Hospital + UHS Attack](#)
[Rogue Shopify Employees Steal Data from 200 Stores](#)
[Memory Replay to Overcome AI "Catastrophic Forgetting"](#)
[G2M Research 2021 Webinar Schedule](#)

Ransomware Attack Intended for University Hits Hospital + UHS Attack

A [cyberattack](#) on a hospital in Germany left a woman dead after equipment failures resulted in a shutdown of the emergency room, with patients diverted to another facility twenty miles away. The woman died on the hour-long drive to the second facility. The attack will be treated as a homicide if medical examiners determine that her death was the direct result of the diversion.

[Thirty servers](#) at the hospital were encrypted and a ransom note left on one of the servers, with no specific amount of money, addressed to Heinrich Heine University, which is affiliated with the Huesseldorf Hospital. The attackers stopped the attack once they realized they had mistakenly attacked the hospital.

This past weekend, one of the largest healthcare providers in the United States, [Universal Health Services](#), was hit with a [ransomware attack](#). Computer screens changed to text

referencing a "shadow universe" which is consistent with Ryuk ransomware. UHS operates more than 400 hospitals in the US and UK and serves millions of patients each year.

Ryuk ransomware is linked to Wizard Spider, a Russian cybercrime group according to Crowdstrike. The group goes "big game hunting" targeting large organizations, including the US Coast Guard. Some ransomware cybercriminals pledged not the attack health organizations and hospitals during the pandemic but Ryuk has not agreed to back off.

And, despite any "pledges" to back off during the pandemic, a report from Microsoft indicates that attacks against hospitals have increased. Microsoft has been tracking REvil as part of a broader monitoring of human-operated ransomware attacks, finding a trend among attackers to repurpose old tactics to take advantage of the health crisis. REvil exploits gateway and VPN vulnerabilities:

> Adversaries behind these attacks exhibit extensive knowledge of systems administration and common network security misconfigurations, which are often lower on the list of "fix now" priorities. Once attackers have infiltrated a network, they perform thorough reconnaissance and adapt privilege escalation and lateral movement activities based on security weaknesses and vulnerable services they discover in the network. In these attacks, adversaries typically persist on networks undetected, sometimes for months on end, and deploy the ransomware payload at a later time. This type of ransomware is more difficult to remediate because it can be challenging for defenders to go and extensively hunt to find where attackers have established persistence and identify email inboxes, credentials, endpoints, or applications that have been compromised.

One consequence of the UHS attack - at a Pennsylvania psych facility, nurses asked patients what medications they take for morning medications and did not distribute the evening medications because there are no records available without access to computers. Nurses were frustrated at having to handwrite patient notes.

And, I can't help but wonder what Jack Nicholson ("One Flew Over The Cuckoo's Nest") just requested for his morning meds.
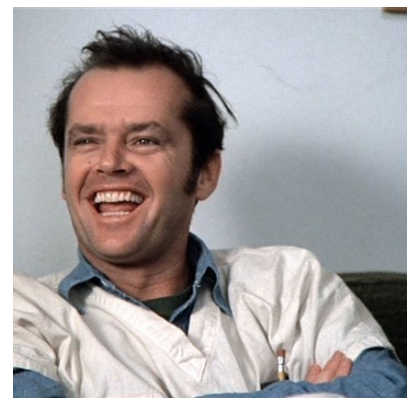
Cybersecurity Wisdom-

"Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers." Chris Pirillo

Two rouge members of Shopify's support team accessed customer data from 200 merchants, and is the third incident of a "malicious insider" in the past month. Shopify terminated the employees and is working with the FBI to aid in the criminal investigation. In July, Shopify reported skyrocketing earnings due to a surge in online sales. Lisa Forte, partner at Red Goat Cyber Security LLP, said insiders are rare but their dangers lies in their unique access, and:

> Incidents involving insiders are also hugely damaging from a reputational standpoint. Perhaps more so than other attacks. Shopify have acted quickly and apparently transparently so far. It is unclear at this point what the precise motive of these insiders was, but all insider threats fall into one of three categories: fraud, sabotage or theft. Often insiders are not working totally alone, with research evidencing the tendency of colleagues to notice but ignore suspicious behavior.

Shopify issued a statement saying they have "zero tolerance for platform abuse and will take action to preserve the confidence of our community and the integrity of our product."

Memory Replay to Overcome AI "Catastrophic Forgetting"

The "Achilles" heel of artificial learning is called "catastrophic forgetting" and refers to the inability of AI algorithms to incorporate memory for inference. A basic example is the ability of a child to discern a cat from a dog and later apply that knowledge to other animals, finding similarities and distinctions.

> An artificial neural network learns by adjusting synaptic weights - how strongly one artificial neuron connects to another – which in turn leads to a sort of "memory" of its learnings that's embedded into the weights. Because retraining the neural network on another task disrupts those weights, the AI is essentially forced to "forget" its previous knowledge as a prerequisite to learn something new. Imagine gluing together a bridge

made out of toothpicks, only having to rip apart the glue to build a skyscraper with the same material. The hardware is the same, but the memory of the bridge is now lost.

When training a robot to climb stairs then turn off a light, the robot will overwrite the configuration used to climb the stairs to optimize performance of turning off the light.

USC Viterbi Professor Paul Bogdan explains, "the brain's networks have an extraordinary capacity to minimize latency, maximize throughput and maximize robustness. This means that neural networks negotiate with each other and connect to each other in a way that rapidly enhances network performance." Bogdan and his team are using multifractal analysis and quantitative phase imagining to model brain performance for use in AI. This application has benefits for detecting cancers in early stages

Uber AI Labs and the University of Vermont developed ANML, a neromodulated meta-learning algorithm, which is able to learn 600 sequential tasks with minimal catastrophic forgetting. Jeff Clune, now OpenAI research scientist, lauds this accomplishment, "This is relatively unheard-of in machine learning. To my knowledge, it's the longest sequence of tasks that AI has been able to do, and at the end of it, it's still pretty good at all the tasks that it saw."

A potential work around is "memory replay."

Researchers from University of Massachusetts Amherst and Baylor University propose a new memory replay approach rather than simply storing previous examples and replaying them when learning something new. The approach of replaying many examples to enhance learning is highly inefficient and requires storage of massive amounts of data. The new approach mimics the brain – the brain does not store data.

"Abstract generative brain replay" approach involves replaying a representations of memories to learn new ones. The brain generates abstract representations of memories, with less detail, and provides a more systematic, streamlined approach to learning. Gido van de Ven explains, "Our method achieves state-of-the-art performance on challenging continual learning benchmarks without storing data, and it provides a novel model for abstract level replay in the brain."

"Computers will overtake humans with AI within the next 100 years. When that happens, we need to make sure the computers have goals aligned with ours."

Stephen Hawking
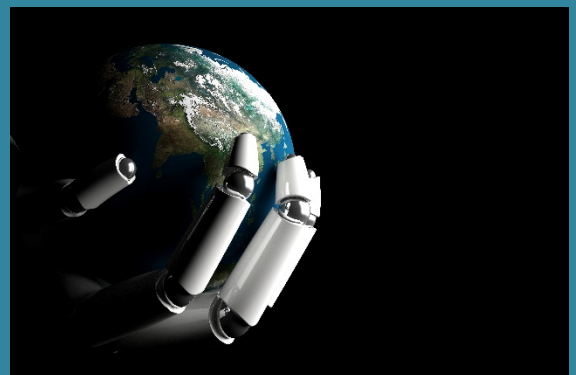
G2M Research Webinar, Tues, October 20, 9am- register here

AI, GPUs, and Storage Use Cases in Healthcare

Upcoming AI/ML & Cybersecurity Events - All Virtual

Oil & Gas Cybersecurity Summit, Oct 2-10

ISC West, Oct 5-7

EAI International Conference on

Digital Forensics & Cyber Crime, Oct 15-16

Open Data Science Conference, Oct 27-30

AI & Big Data Expo, Nov 5-6

G2M Research Webinars – 2020 and 2021

As our industry continues to be virtual, webinars can be a good way to stay up to date and get your message out. G2M has several webinars scheduled for this year on hot topics in our industry. Interested in attending our webinars? Register by clicking on the dates of interest. Interested in Sponsoring a webinar? Contact **G2M** for a prospectus.

Our September webinar "Edge Computing - Get (and Keep) Your Data Off Of My Cloud" was sponsored by Lightbits Labs (Josh Goldenhar), Scaleflux (JB Baker), and NGD Systems (Scott Shadley). View the recording and/or download a PDF of the slides here.

2020 Webinars

Oct 20:   AI, GPUs, & Storage Use Cases in Healthcare

Nov 17:   Implementing NVME™ & NVMe-oF™ for Cloud Service Providers

2021 Webinars

Jan 19:   Can Your Server Handle the Size of Your SSDs?

Feb 23:   Storage Architectures to Maximize the Performance of HPC Clusters

Mar 23:   One Year After COVID-19: How did Storage Architectures Perform for Biotech AI Modeling and What Can We Learn From This?

April 20:   The Race to be Relevant in Autonomous Vehicle Data Storage (On-Vehicle and Off-Vehicle)

May 18:   Responsive & Efficient Storage Architectures for Social Media

June 15:   Where has NVMe-oF™ Progressed to in 2021

July 13:   Computational Storage vs. Virtualized Storage in the Datacenter: And the Winner Is"?

Aug 17:   AI/ML Storage: Distributed vs. Centralized Architectures

Sept 14:   Composable Infrastructure vs. Hyper-Converged Infrastructures for Business Intelligence

Oct 12:   Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?

Nov 9:   The Radiometry Explosion: Can Storage Keep Pace?

Dec 14:   2021 Enterprise Storage Wrap-Up Panel Discussion

G2M COMMUNICATIONS

Effective Marketing & Communications with Quantifiable Results