The Daily Hacker:

Pivot & Bytes

Wednesday, September 29, 2021

What's Inside:

- **Welcome to the Conference from Judy Darwin**
- **Conference Happenings**
- **Technical Track Feature Article: "Lessons Learned: COVID 19 Cyber Impacts"**
  - **Dr. David Schippers-Walsh College**
- **Today's Feature Blog Post: "Fight AI with AI"**
  - **Joshua Crumbaugh, Chief Hacker/CEO, PhishFirewall™ PeopleSec®**
- **"Preparing a Future Cyber Workforce: Teaching Students Through Experiential Learning"**
- **Did You Know? *Fun Facts***

Welcome to the NCS Conference from the Director of the National Cyber Summit and President of the Southeastern CyberSecurity Foundation. (SCSF), *Judy Darwin-NASA*

Welcome to Huntsville, Alabama, and the 12th Annual National Cyber Summit, *Cybersecurity 2021: Pivot, Respond, Inoculate*, hosted by Cyber Huntsville (CH) and North Alabama Chapter of ISSA (NAC-ISSA). We are honored that you have chosen to attend this year's summit. NCS is the nation's premier cyber security-technology event, offering unique educational, collaborative and workforce development opportunities for industry leaders and the next generation of innovators.

We would like to thank all our 2021 Diamond sponsors, Accenture, All Points, Colsa, ECS, FBI, Intuitive, RockITek, and System High as well as our Platinum Sponsors, Dynetics, Gray Analytics, ManTech and Noblis for their support. NCS appreciates the support of many other sponsors to bring the most attended conference to date.

Our agenda is full of subject matter experts from across cyber field of advance manufacture, research and development to Governance and Compliance. NCS will showcase innovative research and technologies that are changing the face of cyber industries. We hope you will enjoy the compelling speakers, see the latest cyber-technology industry trends, learn new skills, and share tips and tricks among peers. We have two Technical Tracks, Forensics Track, Advanced Manufacturing Track, Redstone Eco-System Track, and Research Track.

Be sure and sign up for additional activities we are bringing this year, a Cyber Escape room from Living Social, Women's Breakfast, as well as time honored events including the two Lightning Rounds, and Show Floor Stage Panel Discussions. The Cyber Cup Challenge held on the exhibit floor is sponsored by Deloitte.

We are partnering with Destination Huntsville this year to bring after hour Huntsville "boots on the ground" experiences for those who are visiting Huntsville for the first time, but also fun for local community to learn about happenings and fun places to eat, drink and be merry.

We will be having an OKTOBERFEST after hours' event hosted by SENTAR at The Nook downtown Huntsville Wednesday Evening from 5-7 PM. The Nook is located at 3305 Bob Wallace Avenue.

Our all-volunteer Blue Team members have been working over the past 18 months, to bring what we believe, the best conference in our 12-year history! We continue to incorporate new tracks, activities and events to bring you the best possible conference experience. This year is no exception! From hearing to subject matter experts, networking opportunities, Cyber Escape Room to the Cyber Cup Challenge, we have something for everyone.

If you are interested in joining Cyber Huntsville https://cyberhuntsville.org/sys/website or NAC-ISSA North Alabama ISSA – North Alabama Chapter of Information Systems Security Association (nac-issa.org), we can find a place to connect you to your specific interest. Both organizations offer leadership roles, networking opportunities, and training sessions and more. Be sure to visit our booth and find out how to get involved.

I personally would like to thank the Blue Team Volunteers that have so passionately participated in countless meetings, actions, and changes of postponing to starting back up again. They all have keep the ball rolling to make the NCS 2021 the success it is today: Nisheeth Agrawal, Stacie Bohanan, Katie Bosarge Patterson, Erica Bradford, Larry Burger, Joanna Centola, Jason Cuneo, Paul Daymond, Ben Denton, Barbara Fast, Rob Goldsmith, Greg Harris, Ted Henrich, Felisa Jackson, Kim King, Dr. Kim LaFevor, Phillip Lee, Ernest McLamb, Jamie Miller, Mona Miller, Tommy Morris, Nichole Obrien, Cary Pool, Stephen Pratt, Marcus Sachs, Ron Sikes, and Rachel Smith.

As we look back at the past year, we recognize the importance of taking this time to ***Pivot*** from our security practices that do not serve us well, ***Respond*** promptly to current incidents, ***Inoculate*** and harden our defenses from future attacks.

Thank you for participating in this year's NCS2021. We hope you have a wonderful experience and enjoy the many networking opportunities provided to you!

Sincerely,

2021 National Cyber Summit Director,
President, Southeastern Cyber Summit Foundation,
Judy Darwin

Conference Happenings

Wednesday, September 29th, 2021

What?	When?	Where?
Exhibition Hall Open	**7:00am to 5:00pm**	**Exhibition Hall**
Summit Registration and Information Desk	**7:00am to 5:00pm**	**South Hall Foyer**
Huntsville Street Party	**7:00am to 3:30pm**	**Exhibition Hall, Booth #625**
Networking Breakfast	**7:00am to 8:00am**	**Exhibition Hall**
Cyber Cup Challenge	**8:00am to 12:00pm**	**Exhibition Hall**
General Session: Welcome Remarks	**8:00am to 8:30am**	**East Hall**
Keynote Presentation: *Brian Turner-* Executive Assistant Director, Criminal, Cyber, Response, and Services Branch-FBI	**8:30am to 9:15am**	**East Hall**
Keynote Presentation: *Dr. Raj Iyer-SES* Chief Information Officer, Office of the Secretary of Army	**9:15am to 10:00am**	**East Hall**
Networking Break and Lightning Rounds	**10:15am-10:30am**	**Exhibition Hall** **Stage 1-Next Generation Low-Cost Data Diodes for Physical Cyberprotection** **Stage 2- Ransomware Attacks and Developing a Critical Response Plan**
Networking Break and Lightning Rounds	**10:45am-11:00am**	**Exhibition Hall** **Stage 1-Embedded Systems Pentration**

		Stage 2- Attivo Networks
Keynote Speaker: **Jon "Maddog" Hall** ***"If You Don't Have Free Software You Don't Have S*IT"***	**11:00-11:45am**	**East Hall**
Job Fair	**11:00am-3:00pm**	**South Hall**
Keynote Luncheon: **Lynn Dohm, Executive Director-Women in Cybersecurity (WICYS)**	**11:45-1:00pm**	**North Hall 2**
Networking Lunch	**11:45-1:00pm**	**Exhibition Hall**
Lightning Rounds	**12:00pm-12:15pm**	**Exhibition Hall** **Stage 1-Secure, Reliable Infrastructure Services in the Southeast** **Stage 2-Industrial Control Cyber Threat Hunting**
Lightning Rounds	**12:30pm-12:45pm**	**Exhibition Hall** **Stage 1-The Cloud Developer-Generation DevOps** **Stage 2-Mission Cyber Demonstrator: Visualizing Cyber Risk to Mission Impact**
Cyber Cup Challenge	**1:00pm-5:00pm**	**Exhibition Hall**
Research Track	**1:00pm-5:00pm**	**North Hall Salon**
Main Stage Panel: **Cybersecurity in Critical Infrastructure Panel: Global Threats. Local Impacts.**	**1:15pm-2:15pm**	**Exhibition Hall**
Breakout Track Sessions: Advanced Manufacturing	**1:15pm-2:00pm**	**Ballroom 3**

"Manufacturing Security: The Old New Battleground"-*Sean McCarthy, Booz Allen Hamilton*		
Breakout Track Sessions: Law Enforcement/ Forensics **"That's Secret---Can a Forensic Report be Protected as a Privileged Work Product?"—*Hoyt L. Kesterson II, Avertium & Kimberly Peretti, Alston & Bird, LLP***	**1:15pm-2:00pm**	**Ballroom 5**
Breakout Track Sessions: Redstone Arsenal Cyber Ecosystem **"Understanding CMMC: It's not just a Technical Solution"---*Steven Rivera, Redspin & Dr. Thomas Graham, Redspin***	**1:15pm-2:00pm**	**Ballroom 4**
Breakout Track Sessions: Technical **"Managing on the Spectrum-Getting the Best from Cyber Talent on the Autism Spectrum"—*Teresa Thomas, The MITRE Corporation***	**1:15pm-2:00pm**	**Ballroom 1**
Breakout Track Sessions: Technical **"Who's Got Access? How AI Ends the Left-brain, Right-brain Feud"---Eve Maler, ForgeRock**	**1:15pm-2:00pm**	**Ballroom 2**
Sponsored Session: RocklTek **"Making Adversaries Irrelevant"**	**1:15pm-2:00pm**	**East Hall**

Gary Connor, Brigadier General (USAF-ret) ***Joe Faxlanger, Pkware*** ***Brandon Hoffman, Intel 471*** ***Darren House, RockITek*** ***Adam Rosen, Stealthbits***		
Breakout Track Sessions: Advanced Manufacturing **"How Low Can you Go? Establishing Real-Time Protection Against Level 0 and 1 Control System Cyber Attacks"*---Mark Baggett, Mission Secure***	**2:15pm-3:00pm**	**Ballroom 2**
Breakout Track Sessions: Advanced Manufacturing **"Edge Computing as a Security Tool in ICS/SCADA Systems*"---Eric Dull, Deloitte***	**2:15pm-3:00pm**	**Ballroom 3**
Breakout Track Sessions: Law Enforcement/ Forensics **"Roll Your Own Threat Hunting Environment (for free)" *---Chris Crosby, COLSA Corporation***	**2:15pm-3:00pm**	**Ballroom 5**
Breakout Track Sessions: Technical **"Continuous Monitoring-Transforming Risk Management*"---Nathan Swab, Sentar***	**2:15pm-3:00pm**	**Ballroom 1**
Breakout Track Sessions: Remarks by Paul Puckett	**2:15pm-3:00pm**	**Ballroom 4**

Sponsored Session: System High **"DCIO and SAP IT-Introduction to the Office"** ***Jason "Max" Klimek, Systems High*** ***Michael "Bear" Newsom, System High***	**2:15pm-3:00pm**	**East Hall**
Networking Break and Lightning Rounds	**3:00pm-3:30pm**	**Stage 1-MARS Suite-Cyber Common Operating Picture Solution**
Breakout Track Session: "Evolving and Emerging National Security Threats from China"—*Jay Town, Gray Analytics*	**3:15pm-4:00pm**	**Ballroom 1**
Breakout Track Sessions: Law Enforcement/ Forensics **"Hunting Modern Threat Actors"—*Dr. Vinny Troia, Night Lion Security***	**3:15pm-4:00pm**	**Ballroom 5**
Breakout Track Sessions: Redstone Arsenal Cyber Ecosystem **"Cyber Resiliency as a Key Element of Holistic Aircraft Survivability"—*Tom Barnett, DEVCOM***	**3:15pm-4:00pm**	**Ballroom 4**
Breakout Track Sessions: Technical **"Malware Autopsy: Reverse Engineering a COVID-19 Email Attack"—*Dr. Wesley McGrew, MartinFederal Consulting LLC***	**3:15pm-4:00pm**	**Ballroom 4**
Sponsored Session: Accenture	**3:15pm-4:00pm**	**East Hall**

"Enhanced Cyber Operations with CTI and AI" ***David Dalling, Accenture Federal Services*** ***Michael Goodman, Accenture Federal Services*** ***Howard Marshall, Accenture Federal Services***		
Breakout Track Sessions: Advanced Manufacturing **"Cybersecurity and Bridging the Weakest Link: Integration of People and Processes"—** ***Dr. Dave Schippers, Walsh University***	**4:15pm-5:00pm**	**Ballroom 3**
Breakout Track Sessions: Law Enforcement/ Forensics **"MITRE Engage: MITREs Thoughts on Cyber Denial, Deception, and Adversary Engagement"—*Dr. Stanley Barr, MITRE & Maretta Morovitz, MITRE***	**4:15pm-5:00pm**	**Ballroom 5**
Breakout Track Sessions: Technical **"Banes of a Pentester-Overly-Common, High-Risk Enterprise Vulnerabilities and How to Remediate Them"—*Cornel du Preez, Abricto Security***	**4:15pm-5:00pm**	**Ballroom 1**
Breakout Track Sessions: Technical **"Evaluating Intrusion Detection Systems in the Absence of Robust Datasets"—*Reece***	**4:15pm-5:00pm**	**Ballroom 2**

Johnston, DESE Research, Inc.		
Sponsored Session: Intuitive **"Modern Cyber Economics and Delivery Models"—** ***Chuck Speaks, Intuitive Research and Technology Corporation***	**4:15pm-5:00pm**	**East Hall**
General Session: "Countering Adversaries in a Dynamic Cybersecurity Environment"—*Sid Kaul, All Points*	**4:15pm-5:00pm**	**Ballroom 4**
After Hours Social Event **Loosen your Lederhosen and join Sentar for an Oktoberfest Celebration! Beer, Brats, and Music!**	**5:00 pm-7:00pm**	**Location: The Nook 3305 Bob Wallace Ave SW, Huntsville**

Due to the present dynamic environment, some sessions may be subject to change. For the most up-to-date schedule with any changes can be found on the following QR Code.

Scan this QR code to see the detailed agenda and/or the speaker information

Lessons Learned: COVID19 Cyber Impacts

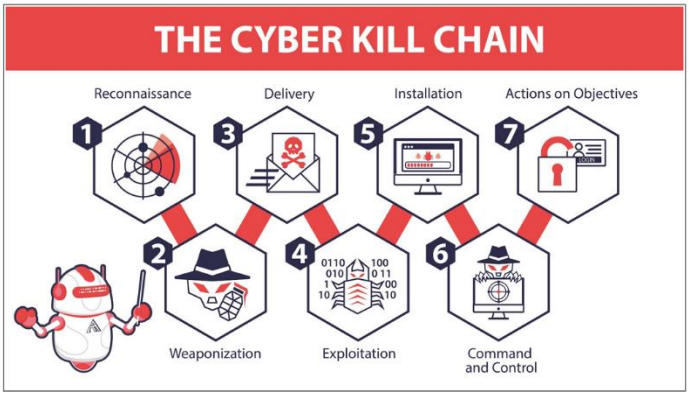
By Dr. David Schippers, CyberAutomotive Program-Walsh College

Introduction

While COVID-19 spread across the globe in 2020, the United States (U.S.) Health and Human Services (HHS) was hit with a cyber-attack [1]. John Ullyot, from the National Security Council, indicated the attack attempted to impact HHS responses to the COVID-19 crises. During COVID-19 in Asia, another group, dubbed Advanced Persistent Threat (APT) 36 and believed to be associated with Pakistan, launched a spear phishing campaign with a fake health advisory masquerading as an official communication from the government of India [2]. Other groups, including Vicious Panda, Mustang Panda, Kimsuky, Hades, Emotet and Lokibot, employed COVID-19 lures to compromise targets [2].

Massive global issues and problems are often leveraged to create compromises and scams by state-sponsored threat actors and cyber criminals. The threat to HHS from APT36 is a prime example of threat actors' tenacity to leverage fear, misinformation and hysteria for gain. Over the course of the COVID19 pandemic, a number of lessons can be gleaned for organizations to enhance and increase security postures. Within this article, definitions on cybersecurity terms will be presented, lessons learned associated with cybersecurity, some industry trends, resiliency recommendations and final thoughts.

Terms Cyber Kill Chain



The first term for the lessons learned discussion is the cyber kill chain. The cyber kill chain was popularized by Lockheed Martin, defining the framework of exploitation and approach to cybersecurity compromises. As seen in Figure 1, attackers begin with reconnaissance. With data, attackers determine the best approaches to attack and infiltrate an organization, often referred to as weaponization. With an attack methodology defined, attack payloads are created and delivered to be effective. If a payload/attack is successful, exploitation of the targeted process, human or vulnerability is completed. Attacker move to install additional tools to "phone home" and take direction from command-and-control infrastructure. One inside your network, attackers continue to move on their objectives.

Figure 1. Obtained from [3].

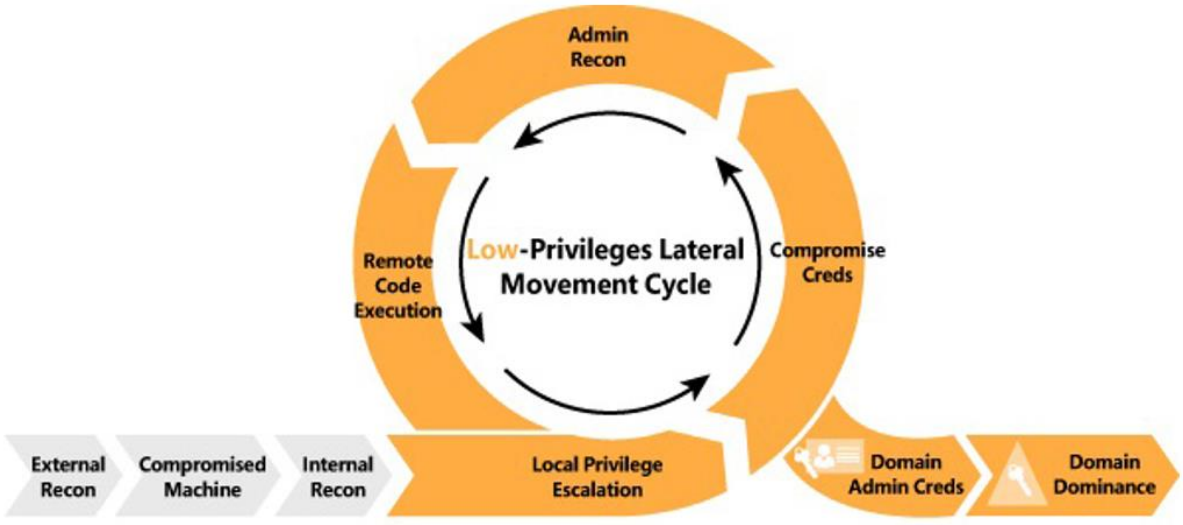


Figure 2. Infrastructure Pivot. Retrieved from [4]

As seen in Figure 2, attackers pivot through your infrastructure and security measures to gain more access. Pivoting involved lateral movement through your infrastructure to gain administrative access and domain administration credentials. If an attacker can gain administrative domain credentials, the attacker gain domain dominance, which spells certain doom for most organizations.

The cyber kill chain is effective for a number of reasons. First up, cybersecurity implementations often assume assets, such as laptops and desktops, within our infrastructure are trusted because they are within our domain. Cybersecurity implementations are often layered, but trust is inherently assumed, depending on the asset's location within our defined infrastructure. For example, the existence of a demilitarized zone for our network indicates higher levels of trust, depending on an asset's location. In the context of protecting our infrastructure, we focus on the "attack surface", attempting to mitigate vulnerabilities. The cyber kill chain exploits these trust levels by finding a way in. Once an attacker has gained access within a trust area, pivoting and continued lateral movement is easier to accomplish. In essence, once the attacker breaches the gates, their level of effort diminishes with new level of trust gained. This brings us to the next definition: Zero Trust

Zero Trust

Zero trust flips our cybersecurity posture. Instead of presuming there are trusted networks, devices or people, everything is monitored and assumed untrustable. (Please realize, we're discussing this at a high level.) Instead of an "attack surface", zero trust defines and focuses on the most important aspects of your infrastructure or a "protect surface". Zero trust shifts from protecting everything to shifting to cyber resiliency, focusing on allotting limited resources to the most important assets/systems. There is a cost with additional monitoring for trust violations, but elevated trust monitoring across the enterprise can directly impact the cyber kill chain approach of attackers.

Risk, BCP & DRP

Most organizations create business continuity plans (BCP) and disaster recovery plans. Business continuity plans focus on ensuring your organization and operations continue to function during adverse events. Disaster recovery plans (DRP) address recovery of operations due to loss or interruptions. Both of these plans intend to identify potential risks, weaknesses and threats against ongoing organizational operations. BCP and DRP rely heavily on an organizations ability to operate mature processes under adversity.

Mature Processes

Mature processes are critical to successful organizations. The Department of Defense issues the Cybersecurity Maturity Model Certification for the cybersecurity requirements associated with operating within the DOD supply chain. CMMC is impactful and impressive due to its clear delineation of the organizational skill and maturity required to address and combat top threats. CMMC defines different skills levels associated with different levels of maturity [5]; skills increase in complexity as an organization works up the levels. Although organizations typically begin in Level 1, which means they illustrate generic cyber hygiene and basic compliance approaches, CMMC defines a road map for organizations to level up their cybersecurity and cyber resilience skills [5]. Level 5 is the ultimate goal. CMMC focuses Level 5 on standardization and optimization across the organization. Level 2 documented and established procedures. Level 3 merged resource allocation and documented practices and processes. Level 4 layered in performance metrics. Level 5 brings the feedback loop or lessons learned. Similar to an incident response lesson learned, organizational leadership regularly evaluates metrics, vision, goals, requirements, and allotted resources. Level 5 implies a clear, systematically managed and operated cybersecurity process, including ongoing oversight and updates to ensure evolving risks and threats are anticipated and addressed [5]. Mature process levels define our level or response against a level of risk. In short, the lower level of your process maturity, the lower your capability to respond. Your response capability is also impeded by your ability to adapt to the Fog of War.

Fog of COVID-19

The Fog of War is the amount your situational awareness is clouded during adverse events. The Fog of War is most often associated with military operations. In cybersecurity attacks or other adverse events, the gravity, depth and severity of impact can create adverse conditions, resulting in lowering cognitive abilities, adaption and overall capabilities during the adverse event. COVID19 created societal conditions of panic and fear, resulting in a version of the Fog of War. As fear, uncertainty and stress increase, confusion, impatience and panic impede our ability to make rational and objective decisions.

Just as the Fog of COVID19 took off, attackers moved to exploit a number of factors: cultural and organizational uncertainty, increased security misconfigurations, remote workforce vulnerabilities and supply chain disruptions. Attackers did what they do best, leverage your weakness to their advantage.

Lessons Learned

Communication

One of the first lessons learned is communication vulnerabilities. Attackers knew interest and desperation for information on the pandemic would be very high. Cyber-attacks grew by 400% in the first few months of the pandemic. Phishing emails were the primary tool, often impersonating a trusted source, such as a government or international agency. Attached documents included malicious payloads for exploitation of targets.

Immature Processes

The next lesson learned is exploitation of immature processes. As organizations struggled to maintain continuity during the pandemic, remote workforces were deployed. Virtual private network expansions were required to handle the bandwidth of entirely remote workforces. As organizations deployed quickly, any lack of process or defined security configurations resulted in ad hoc decision making. Any variance in settings can result in security measures being disabled. Attackers knew large organizations normally well protected would most likely have gaps arise.

Unpatched Vulnerabilities – Home Networking Equipment

An extension of the remote workforce lesson learned was unpatched equipment allowed into the zone of trust. Home equipment is not patched or maintained at the same security level or consistency of enterprise class equipment. Attackers knew with a massive transition to remote workforces, old vulnerabilities not normally exploitable would be back on the table with unpatched/unmaintained home equipment allowed into the zone of trust. Looking back on summer of 2020, Honda, Garmin, Twitter and Canon all suffered breaches in a three-month period, suggesting normal stalwarts of security fell victim to the Fog of COVID19.

Enter Doxware

Beyond standard ransomware, a new trend evolved during the pandemic: doxware. Doxware, or when attackers notify your customers you have been breached if you fail to pay a ransom, emerged from ransomware trends in 2020. Ransomware is malicious software that locks system data, requiring a ransom to unlock the data. Reliable and consistent backups are significant strategies to combat ransomware, allowing the organization to reload data instead of paying a ransom. Attackers know organizational brand and trust are critical for business success. As businesses quit paying ransoms, attackers evolved their approach to blackmail businesses into paying. If the business doesn't pay the ransom, attackers may sell the locked data, notifying customers of the breach shaming the business and tarnishing their brand [6].

Industry & Regional Trends

For each industry and region presented, key information is presented for decision makers to consider with cybersecurity positioning. Of special note, Education and Government industry experience high levels of social engineering. In Education, social engineering employs pretexting 80% in the reported cases. In Government, social engineering employs only one percent of pretexting in the reported cases.

Table 1. Industry Trends.

Industry	Threat Actors (External – E Internal - I		Attacker Motives (Financial- F Espionage – E)		Attacks Leveraged	Top Defense
Healthcare	E-61%	I-39 %	F-91%	E-4%	1) Misdelivery 2) Publishing 3) Misconfiguration	Security Awareness, Secure Config
Education	E-80%	I-20%	F-96%	E-3%	1) Social Engineering 2) System Intrusion 3) Miscellaneous Errors 4) Basic Web App Attacks	Security Awareness
Entertainment	E-70%	I-30%	F-100%		1) Stolen Credentials 2) Other 3) Ransomware 4) Misconfiguration 5) Phishing	Security Awareness, Secure Config
Government	E-83%	I-17%	F-96%	E-4%	1) Social Engineering 2) Miscellaneous Errors 3) System Intrusion 4) Basic Web App Attacks	Security Awareness, Access Control
Manufacturing	E-82%	I-19%	F-92%	E-6%	1) Ransomware 2) Other 3) DoS 4) Phishing 5) Stolen Credentials	Security Awareness, Secure Config

Adapted from [7]

Big Game Hunters

In recent years, malware as a service increased, being provided by illicit players avoiding the risk of carrying out attacks. These service-based providers enable the big game hunters (BGH). BGH are the advanced persistent threat groups coordinating large and impactful attacks, taking on the risk of being caught [8]. In 2019, a few BGH leveraged doxware. During the pandemic, Twenty-three BGH adopted the data extortion/doxware approach, leveraging data leak sites [8]. Doxware increased significantly during the pandemic, jeopardizing any organization leveraging backups or other mitigations to paying ransoms.

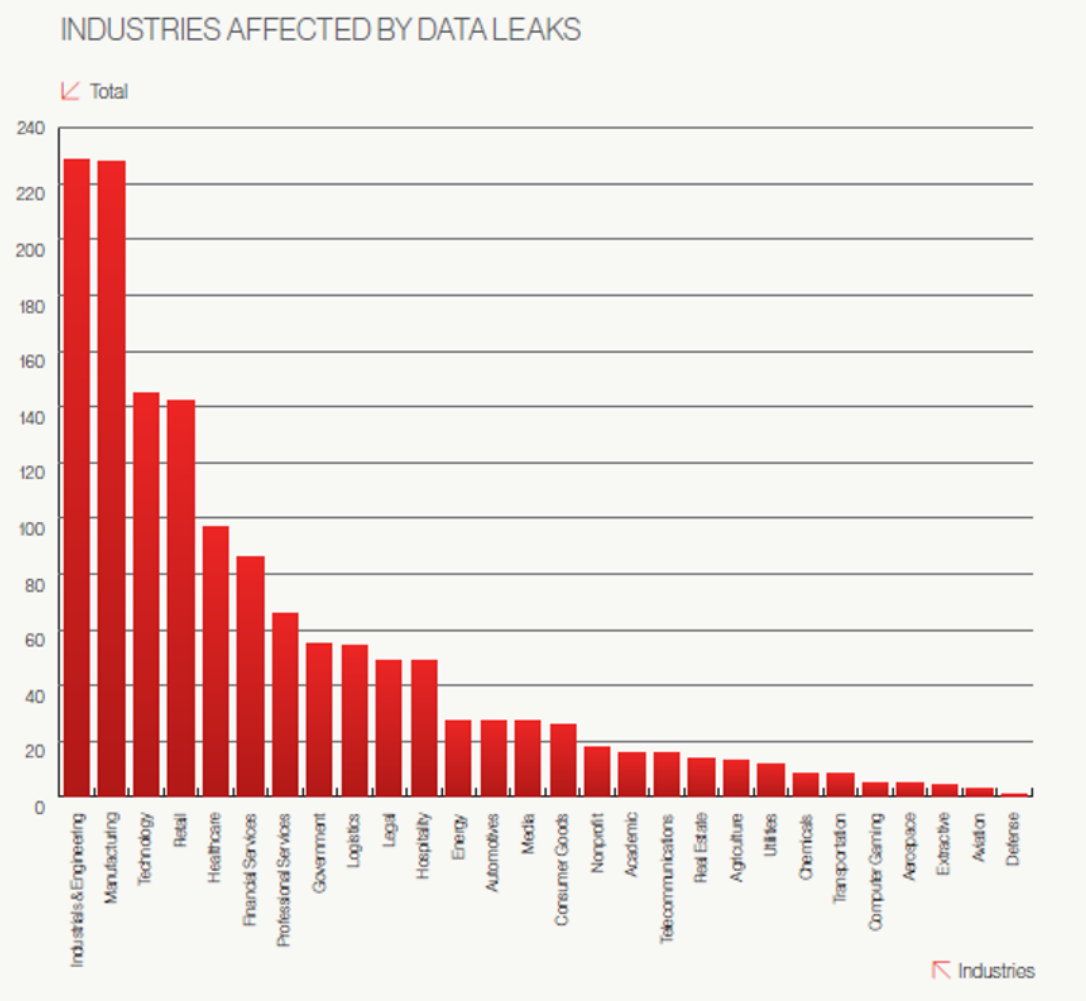


Figure 3. Data Leaks & Doxware. Retrieved from [8].

Figure 3 illustrates the top industries impacted by data leaks and extorsion. Of note, Industrial & Engineering and Manufacturing tie as the top two affected. If your organization operates in an industry listed, risk management and incident response plans should integrate doxware considerations.

Cybersecurity & Resiliency Recommendations

As leader consider all of the events, shifts and lessons in cybersecurity from the COVID-19 accelerator, there are five critical investments organizations should implement (Microsoft). Many of the recommendations provided are not new. Ironically, COVID-19 highlighted the importance of these technical approaches to improving overall cybersecurity and cyber resiliency postures. The recommendations are:

1. Multifactor Authentication
2. Endpoint Device Protection
3. Anti-phishing Tools
4. VPNs
5. End-user Security Education [9]

Beyond Microsoft recommendations, organizations should investigate and consider implementing zero trust models. With zero trust shifting organizations to a cyber resiliency position, it is a larger technical implementation, requiring mature processes.

Beyond technical implementations, highly resilient organizations were studied and determined to have three critical skills/abilities. These skills separated resilient organizations from others. (These skills align with the CMMC model.) These skills are:

1. Organize & Deploy Resources
2. Communicate Regularly
3. Coordinate Responses [10]

In the context of COVID-19 response, resilient organizations leveraged their ability to deploy their resources and people through their mature processes. During challenging pandemic responses, organizations with mature processes benefited from leveraging the skills and maturity of their staff and processes to implement alterations effectively and quickly.

In addition to implementation, resilient organizations leveraged their mature communication processes to keep the entire organization informed and aware. Beyond communicating change, mature communication process enables users to comprehend who should be communicating critical change approaches, enabling phishing and social engineering to be spotted quickly.

Lastly, mature processes lead to a system thinking for responses. Leaders understand response decisions create collateral impact to other processes. Risk, response and collateral impact enable proactive thinking for response thinking. Overall, coordinated responses are a mature process considering larger and down channel impacts for the best organizational posturing and approach.

COVID-19 has been catalyst for change. Every organization's process maturity, business continuity and disaster recovery plans were battle tested during the ongoing pandemic. Each organization is in a unique position to determine the efficacy of their cybersecurity posture, approach and resiliency. The only question is – will your organization improve from the lessons learned or simply continue on?

References

1) S. Stein and J. Jacobs, "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak," 16 March 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.. [Accessed 19 March 2020].
2) Threat Intelligence Team, "APT36 jumps on the coronavirus bandwagon, delivers Crimson RAT," Malware Bytes Lab, 16 March 2020. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/. [Accessed 19 March 2020].
3) Retrieved from https://miro.medium.com/max/3200/0*_XXoLka6WzhSLYkl
4) Retrieved from https://ptgmedia.pearsoncmg.com/images/chap1_9780135752036/elementLinks/F01XX01.jpg
5) Carnegie Mellon University and The John Hopkins University Applied Physics Laboratory, LLC, "Cybersecurity maturity model certification (CMMC)," 2020.
6) Whitmore, W. & Parham, G., (2020, June), COVID-19 cyberwar: How to protect your business, Armonk, NY: IBM.
7) https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf
8) https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
9) https://www.microsoft.com/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security/
10) https://www.ibm.com/downloads/cas/Y5QGA7VZ

Today's Feature Blog Post-

Fight AI *With* AI: Automated Spear Phishing Attacks Powered by Artificial Intelligence

By Joshua Crumbaugh

In the world of cybersecurity, it's a never-ending battle. Hackers are always finding new ways to break through your defenses and steal your data. But now they're using AI to do it. This blog post will explore how hackers are using AI for phishing scams so you can stop them before you're the next victim.

Spear phishing continues to be the greatest threat organizations big and small alike face, as it is hard to keep up with all the new scams and tricks. The trouble lies in not just identifying these attacks but stopping them before they happen. Understanding how these schemes work can be very beneficial and is strategically imperative!

The next generation of hackers are using artificial intelligence as a force multiplier to craft spear-phishing emails that appear as if they're from established corporations, such as Amazon, Netflix or your company. 100% of Fortune 50 companies have acknowledged this as the greatest current threat facing their organizations in protecting themselves against spear phishing attacks.

Hacking has been around for a long time, but it's never been more appealing. Hackers exploit people using OSINT (open-source intelligence) or information publicly available on the internet about victims and organizations to automatically target individuals in a provoking psychological manner to infect victims with malware and ransomware. As we all know, these attacks can be financially and reputationally ruinous.

The problem is that hackers have figured out how much value AI can add to their phishing scheme. As you may know, it's often an easy win for attackers if any organization falls victim and gets fooled by this kind of scam. To protect against AI phishing, we must use it as a countermeasure. A recent study found that hackers are actively using machine learning and deep fakes to hack organizations through spear-phishing attacks.

I'm an academic peer-reviewed published author on this subject and have conducted extensive research on preventing phishing attacks. My biggest takeaway is that the best way to prevent attacks is by simulating them with just in time education where you apply science and learn from experience, or rather "use your mistakes as feedback for future endeavors." This creates what I like to call "human virus definitions," and it's great because when these flags pop up, the subconscious tells users that there is an incoming threat. When this happens people rarely question their subconscious, so they move on without giving it thought. This is the best way to get results and it's scientifically proven.

Cybersecurity awareness is not as complex as it may seem. We're just making the problem harder than it needs to be with our outdated learning tactics that are based on methodologies from decades ago. Let’s be honest, awareness is simply a CMMC compliance checkbox for most of us but if we want people to take cybersecurity seriously, then we need more balance between education and entertainment so they can understand this concept in an entertaining way instead of being bored by something too complex for them to comprehend. I know when I'm planning my education I try to make as fun as possible. And I know what you're thinking: "Edutainment doesn't work!" You’re correct, Edutainment doesn’t work. But true entertainment does! It triggers an emotional response and chemical reaction in the user's brain that anchors the lesson in their memory. I believe that if the subject matter is essential, it should trigger an emotional response.

The bad guys have always been a few steps ahead of the defenders, and this time is no different. It's not just because they're using new tactics or technology, but also due to their crafty mindset that we should consider when preparing our countermeasures against these threats!

In the end, people are a lot like computers. They're difficult to train and easy to program - because of this, we must use psychology as our countermeasure in order to achieve any tangible results! A lot of research has gone into both learning theory (the science) or behavioral modification techniques which adversaries such as hackers and nation-states will employ against us; there's no other choice but to fight fire with fire if you want victory over these foes...and sometimes even going up against another form of intelligence could help: take an example from ancient Rome where Julius Caesar would fight Gallic warriors not by weaponizing himself, but rather through tactics derived solely from reading their movements on the ground.

Not everyone is the same. The bad guys get this, and that's why they're using AI to target your individuals with tailored messages, and don't be fooled--it's super convincing! So, for me to make my next point, I'm going to have an artificial intelligence write out my closing paragraph.

To do this, I feed it the content of this blog I've written so far, and the AI does the rest. It quickly generates three pieces of copy for me to choose from, and I chose the following…enjoy!

We need to start thinking about security awareness as a proactive measure. The threat of phishing is real, and we can't just be reactive anymore. The problem is that over 95% of malware and ransomware getting into organizations starts with a phishing attack. We need to get organized around phishing and plan an effective strategy to prevent our users from falling victim in the first place, and our users have got to be current on the threats. This means that we have to get them engaged, or our message is lost to deaf ears! If you're not sure where to get started, reach out for help from one of our experts who specialize in the psychology behind cyber threats. You'll learn how to craft an effective strategy that keeps your users safe by understanding their vulnerabilities and respecting them enough to make it easy for them to do what's right when they don't feel like doing anything at all!

The cybersecurity industry is evolving rapidly and cyber-attacks are becoming more sophisticated. Hackers continue to find new ways to exploit vulnerabilities in systems, networks, and applications. This means that there's never been a greater need for organizations of all sizes to be proactive about their security posture before the attack happens. One way you can stay ahead of these threats is by using AI technology like machine learning or deep fakes, which uses neural network algorithms with deep learning techniques to conduct global targeted interactive phishing campaigns at a faster rate than any human could ever do on their own.

When it comes time for your organization's next round of cyber-defense planning, don't forget about how advances in artificial intelligence have changed the game and the need for our methodologies and tools to keep up with the tactics being used by our adversaries.

The internet can be a scary place, and it's not just because you have to worry about people hacking into your computer. There are plenty of scams out there that will steal your personal information or money with the click of a button. You never know what might happen if you don't "think before you click!"

Cheers,

Joshua Crumbaugh
Chief Technology Officer
PhishFirewall

About Joshua:
Joshua Crumbaugh is one of the world's most famous hackers. He's an engaging and internationally respected cybersecurity subject matter expert, published author, and keynote speaker. During Joshua's ethical hacking career, he has never encountered a single network that could keep him or his teams out. He uses these experiences to educate and entertain audiences with real life hacking stories that captivate the audience. His experience in all things social engineering led him to realize something had to change. This realization led him to found PhishFirewall.

About PhishFirewall
PhishFirewall is the world's first fully automated AI-driven anti-phishing solution. We personalize education, training, and phishing simulations to dramatically lower phishing risks. Our product has been designed to help organizations significantly reduce their level of exposure to ransomware attacks by using artificial intelligence insights that find and correct individual phishing vulnerabilities. Unlike other anti-phishing solutions on the market today, our product drives click rates well below 1% - even for those with a high propensity for clicking.

NCS
National
Cyber Summit

Preparing a Future Cyber Workforce:

Teaching Students Through Experiential Learning

Research has shown that students learn in different ways; however, any time you have the opportunity to teach a student to apply their knowledge, it has been proven to help them retain what they have just learned. Experiential Learning is one of the terms used for this type of Learning. At Athens State University, faculty incorporate different types of Experiential Learning into their curriculum.

Experiential Learning is something that the Computer Science and Information Technology faculty are known to incorporate into their classes. With Athens State University being an upper-division institution with many students being non-traditional, many of them don't have the opportunity to attain internships due to the need to provide for their families through the full-time employment they currently hold. Every student that earns a Bachelor's degree in Computer Science or Information Technology is given this opportunity through their Senior Software Project course. These projects can range from research to partnering with outside organizations to develop custom applications or provide a security analysis of their systems. However, even before students get to their Senior Software Project course, they have the opportunity to be exposed to Experiential Learning in other classes.

In particular, with the focus on Cybersecurity, the Security and Management focuses on concepts that a student needs to be familiar with for a foundation in preparing for the Security+ and PenTest+ Certifications. The course teaches students to perform vulnerability testing, Risk Assessment, and penetration testing to allows students to work with programs and tools that enable them to experiment with cyberattack scenarios and ways to mitigate those attacks. In Digital Forensics, labs are integrated into the class to find hidden images, files, and to do steganography exercises. A class in Cryptography teaches students the foundation to understanding problems association to encryption, authentication, and key distribution. The class teaches them how to evaluate protocols and methods to solve these types of problems, and how to build secure software solutions for them. Another class, System Administration and Scripting Languages, allows students to work on a Linux server exposing students to different computer systems. The class also teaches how to write scripts to automate tasks that could otherwise be tedious and time-consuming, which time is of the essence in the scenario of a security breach.

The best people that can speak to this opportunity are Athens State students. The students were asked to reflect on the following question:

How has the use and introduction of different tools and software in the classroom assisted you in being able to understand and connect what you are learning to the work that you will need to conduct in the field of Cybersecurity?

"Several classes that I have taken for my degree have allowed me to build a skillset and essentially a toolbox of knowledge that I understand how it applies to the real world. Classes in Cybersecurity have allowed me to have hands-on experiences through lab simulations that required me to apply the knowledge that I have learned through lectures and readings. Having a hands-on practical experience allows me to practice what I have learned and have an easier time understanding it because I am applying what has been taught. I have also had exposure to different systems, learned about system administration and writing scripts to automate tasks that might otherwise be tedious. One of those assignments included writing a script to find files with a specific server extension and creating a list of where the files were located. In Cybersecurity, I can understand how this would be useful, especially in a situation where an organization might have had ransomware and need to identify which files in their systems have been encrypted." –Christopher Pendergrass

"When learning something new, reading what something is or how it works is, in my experience, best paired with hands-on work. Taking classes that provided scenarios and labs where students can use tools

such as Nmap, Wireshark, and other devices used in the field strengthened the information that I had read in textbooks. They helped me understand how different computer fields work together. Using these various tools in the classroom allowed me to gain practical experience of what I may one day be doing as part of my career." –Justin Blackburn

"The introduction and opportunity to use different tools and software in the classroom have given me insight into the type of work I will be doing when I start my career. The tools and software have made it easier for me to understand the material and emphasize the importance of transferring the knowledge I was gaining with the skill sets I was building. I am a big hands-on learner, so the labs have helped me because I do not just have to remember the information from a textbook. However, I am learning how to properly apply that knowledge in the real world based on given scenarios." –Zacharias Steffen

For more information about the CS or IT programs, please contact:
Dr. Adam W. Lewis
Associate Professor of Computer Science and Program Coordinator
adam.lewis@athens.edu, (256)233-6505
For more information about Experiential Learning at Athens State University, please contact:
Professor Katia Maxwell
Associate Professor of Computer Science and Director of Quality Enhancement Planning
katia.maxwell@athens.edu, (256)233-6526

For more information about Cybersecurity courses, please contact:
Professor Nisheeth Agrawal
Instructor of Computer Science
nisheeth.agrawal@athens.edu, (256)233-6537

Student information:
Christopher Pendergrass: Bachelor's in Computer Science with a concentration in Cybersecurity and a minor in Mathematics (expected graduation May 2022).
Contact: cpender2@my.athens.edu;

Justin Blackburn: Bachelor's in Computer Science with a concentration in Information Security (now called Cybersecurity, expected graduation December 2021).
Contact: jblackb5@my.athens.edu;

Zacharias Steffen: Bachelor's in Information Technology with a minor in Cybersecurity (expected graduation December 2021).
Contact: zsteffen@my.athens.edu

Did You Know? Fun Facts.

[put a cloud or some outline around Did you Know?]

Huntsville Metro is the #1 Best Affordable Place to Live in the U.S. (U.S. News & World Report, 2020)

Huntsville ranks #18 in the Best Cities to Start of Career in the U.S. (Wallet Hub, 2021)

There are 16 counties in the North Alabama Region with a population of 1.3 million people. The economy is strong and growing (Huntsville Madison County Chamber)

Note from the Editor-

It is so great to have everyone back *'in person'* at our conference this year! In the interest of making our conference even more special for this return, we thought it might be of interest to our attendees to have a daily conference newsletter. So, we are piloting something a bit different this year and debuting a new conference publication titled, "*The"Daily Hacker: Pivot & Bytes*."

This publication brings together information about the hosts of the event: 1) National Cyber Security Summit Foundation, 2) Cyber Huntsville and 3) NAC-ISSA describing the organizations and how you can get involved, as well as a full listing of Conference Happenings, Feature Technical Articles and Blog Posts, as well as 'Fun Facts' about our community and state.

We hope you enjoy this new publication! Also, we are greatly interested in your feedback about this *new addition* to our conference offerings.

Best,

Dr. Kim LaFevor, DBA, SHRM-SCP, SPHR, IPMA-SCP, NDCCDP
National Cybersecurity Summit Foundation-Board of Directors
Senior Executive to the President for Strategy & Innovation-Athens State University

National Cybersecurity Conference Team

Pub Crawl Participating Booths

Tuesday 5:30 - 7:30 p.m.