



# WELCOME TO AUTO-ISAC!

## MONTHLY VIRTUAL COMMUNITY CALL

August 5, 2020

# TEAMS MEETING PROTOCOL

## Please Note...

- 1) The **Microsoft Teams meeting link** will provide both audio and visual presentation. In case you need to dial in for audio, please use the phone number and conference ID provided on the invite in the meeting invitation. If you are outside of the U.S, use “**Local Numbers**” link provided in the same meeting invite.
- 2) If you are dialing in for audio, **please press \*6 to mute or unmute** your line.
- 3) Please keep your **mic muted** at all times, except when the host is addressing your request to ask a question or to provide feedback. Any background noise may disrupt the audio quality for other listeners.
- 4) If you have question or feedback, you can also use the **chat function**.
- 5) If you would like to speak, please use **raise hand function** on your screen. The host will be notified and will acknowledge you when ready.

# AGENDA

Time (ET)	Topic
11:00	<b>Welcome</b> <ul style="list-style-type: none"> <li>➤ Why we're here</li> <li>➤ Expectations for this community</li> </ul>
11:05	<b>Auto-ISAC Update</b> <ul style="list-style-type: none"> <li>➤ Auto-ISAC overview</li> <li>➤ Heard around the community</li> <li>➤ What's Trending</li> </ul>
11:15	<b><i>DHS CISA Community Update</i></b>
11:20	<b>Featured Speaker: Gary Berman, Creator, Cyberheroes Comics</b>
11:45	<b>Around the Room</b> <ul style="list-style-type: none"> <li>➤ Sharing around the virtual room</li> </ul>
11:55	<b>Closing Remarks</b>

# WELCOME - AUTO-ISAC COMMUNITY CALL!

**Purpose:** These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

**Participants:** Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders, and Government – *the whole of the automotive industry*

**Classification Level: TLP GREEN:** may be shared within the Auto-ISAC Community, and “off the record”

**How to Connect:** For further info, questions, or to add other POCs to the invite, please contact us! ([fayefrancy@automotiveisac.com](mailto:fayefrancy@automotiveisac.com))

# ENGAGING IN THE AUTO-ISAC COMMUNITY

## ❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC membership
- ❖ If you aren't eligible for membership, connect with us as a partner
- ❖ Get engaged – *“Cybersecurity is everyone's responsibility!”*

**19**  
*Navigator  
Partners*

**12**  
*Innovator  
Partners*

## ❖ Participate

- ❖ Participate in monthly virtual conference calls (1<sup>st</sup> Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

**20**  
*OEM Members*

## ❖ Share – *“If you see something, say something!”*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

**36** *Supplier &  
Commercial  
Vehicle Members*

*Membership represents **99%**  
of cars on the road in North  
America*

*Coordination with **23**  
critical infrastructure ISACs  
through the National Council of  
ISACs (NCI)*

# AUTO ISAC – 2020 WAY FORWARD

ROLES, RESPONSIBILITIES  
& METRICS

*Measuring  
Success*

## VALUE STREAMS & PERFORMANCE INDICATORS

**Top Line Goal: Zero safety related cyber events in the industry**



### INFO SHARING & AWARENESS

% Participation  
Sharing / Platform /  
Attendance

### EDUCATION

% Taking Educational  
Offerings  
Maturity Surveys

### RELATIONSHIPS

% Member Satisfaction  
with value added  
relationships

**Bottom Line Goal: *Automotive Cybersecurity Resiliency Across Industry!***

# 2020 BOARD OF DIRECTORS

## EXECUTIVE COMMITTEE (EXCOM)



**Kevin Tierney**  
*Chair of the  
Board of the Directors*  
**GM**



**Josh Davis**  
*Vice Chair of the  
Board of the Directors*  
**Toyota**



**Jenny Gilger**  
*Secretary of the  
Board of the Directors*  
**Honda**



**Tim Geiger**  
*Treasurer of the  
Board of the Directors*  
**Ford**



**Todd Lawless**  
*Chair of the  
Advisory Board*  
**Continental**

## 2020 ADVISORY BOARD (AB) LEADERSHIP



**Todd Lawless**  
*Chair of the  
Advisory Board*  
**Continental**



**Brian Murray**  
*Vice Chair of the  
Advisory Board*  
**ZF**



**Kevin Walker**  
*Chair of the SAG*  
**Aptiv**



**Larry Hilkene**  
*Chair of the CAG*  
**Cummins**

# MEMBER ROSTER

## AS OF AUGUST 1, 2020

Highlighted = Change

Aisin	Honda	Oshkosh Corp
Allison Transmission	Hyundai	PACCAR
Aptiv	Infineon	Panasonic
AT&T	Intel	Qualcomm
Blackberry Limited	Kia	Renesas Electronics
BMW Group	Knorr Bremse	Subaru
Bosch	Lear	Sumitomo Electric
Continental	LGE	Tokai Rika
Cummins	Magna	Toyota
Denso	MARELLI	TuSimple
Delphi Technologies	Mazda	Valeo
FCA	Mercedes-Benz	Veoneer
Ford	Mitsubishi Motors	Volkswagen
Garrett	Mitsubishi Electric	Volvo Cars
General Motors	Mobis	Volvo Group
Geotab	Navistar	Waymo
Google	Nexteer Automotive Corp	Yamaha Motors
Harman	Nissan	ZF
Hitachi	NXP	<b>TOTAL: 56</b>



# AUTO-ISAC ACTIVITIES

- Auto-ISAC Member Incident Response Plan (IRP) Review & Drills **Complete**
- Auto-ISAC Member 4 IRP Drills completed - **Complete**
- Debrief on Cyberspace Solarium Commission Report – **August 11<sup>th</sup>**
- Auto-ISAC Europe 2020 Meeting Members & Potential Members only – **September 3&4 – Invitation sent**
- Moving on Vision 2020 incorporating IT/OT – **Starting 4Q20**
- Auto-ISAC Summit **October 14-15<sup>th</sup>** – registration until OCT 30<sup>th</sup>, sponsorships on website – [www.automotiveisac.com](http://www.automotiveisac.com). **VIRTUAL**

**AUTO-ISAC  
SUMMIT**

Oct. 14-15,  
**2020**  
Virtual

**2** days

**400** attendees

**ABOUT THE AUTO-ISAC SUMMIT:**  
The 2020 Auto-ISAC Summit connects global automotive industry insiders during two days of transformative conversations around cyber attack resilience and response.



**Registration Open Until OCT 5<sup>th</sup> || Sponsor Prospectus**

## WHAT'S TRENDING?

*The Auto-ISAC encourages the automotive industry to maintain heightened vigilance to protect ICS and OT systems.*

### NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems

“At this time of heightened tensions, it is critical that asset owners and operators of critical infrastructure take the following immediate steps to ensure resilience and safety of U.S. systems should a time of crisis emerge in the near term... It is important to note that while the behavior may not be technically advanced, it is still a serious threat because the potential impact to critical assets is so high”.

## Noteworthy News

[Garmin's Four-Day Service Meltdown was Caused by Ransomware](#)

[Two More Cyber-Attacks Hit Israel's Water System](#)

[FBI Issues Warning About ELDs](#)

[Getting from 5 to 0: VPN Security Flaws Pose Cyber Risk to Organizations with Remote OT Personnel](#)

For more information or questions please contact [analyst@automotiveisac.com](mailto:analyst@automotiveisac.com)

# CISA RESOURCE HIGHLIGHTS



# 3rd Annual National Cybersecurity Summit

- **The CISA 2020 National Cybersecurity Summit will be held virtually as a series of webinars every Wednesday beginning September 16 and ending October 7:**
  - Sept 16: Key Cyber Insights
  - Sept 23: Leading the Digital Transformation
  - Sept 30: Diversity in Cybersecurity
  - Oct 7: Defending our Democracy
- **No-cost event but pre-registration is required at [https://cisacybersummit2020\[.\]Eventbrite\[.\]com/](https://cisacybersummit2020[.]Eventbrite[.]com/)**
- **More information at [https://www\[.\]cisa\[.\]gov/cybersummit2020](https://www[.]cisa[.]gov/cybersummit2020)**



# CISA Services Catalog

- **Single informational resource on services across all of CISA's mission areas**
- **Covers services available Federal, SLTT, Private Industry, Academia, NGO, Non-Profit, and General Public stakeholders**
- **Intended for electronic viewing from a desktop device only**
- **More information at**  
[https://www\[.\]cisa\[.\]gov/publication/cisa-services-catalog](https://www[.]cisa[.]gov/publication/cisa-services-catalog)
- **Download catalog at**  
[https://www.cisa.gov/sites/default/files/publications/FINAL%20FINAL\\_CISA%20Services%20Catalog\\_20200723\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/FINAL%20FINAL_CISA%20Services%20Catalog_20200723_508.pdf)



# TLP: WHITE – CISA Emergency Directive ED20-03 Mitigate Windows DNS Server Vulnerability from July 2020 Patch Tuesday

- Followed Microsoft’s security update release to address a wormable RCE vulnerability in Windows DNS Server (CVE-2020-1350)
- Action directed at US Federal Departments and Agencies, directive made publicly available for deployment consideration
- Details and resources also made available on CISA’s Current Activities Page
- See:
  - [https://cyber\[.\]dhs\[.\]gov/ed/20-03/](https://cyber[.]dhs[.]gov/ed/20-03/)
  - [https://www\[.\]cisa\[.\]gov/blog/2020/07/16/emergency-directive-ed-20-03-windows-dns-server-vulnerability](https://www[.]cisa[.]gov/blog/2020/07/16/emergency-directive-ed-20-03-windows-dns-server-vulnerability)
  - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2020/07/16/cisa-releases-emergency-directive-critical-microsoft-vulnerability](https://us-cert[.]cisa[.]gov/ncas/current-activity/2020/07/16/cisa-releases-emergency-directive-critical-microsoft-vulnerability)



# TLP: WHITE – CISA Malware Analysis Report - MAR-10292089-1.v1 – Chinese Remote Access Trojan: TAIDOOOR

- The MAR is the result of analytic efforts between the CISA, FBI, DoD, and U.S. Government partners.
- FBI has high confidence that Chinese government actors are using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation.
- MAR includes suggested response actions and recommended mitigation techniques.
- MAR is at [https://us-cert\[.\]cisa\[.\]gov/ncas/analysis-reports/ar20-216a](https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar20-216a)
- STIX-formatted IOCs at [https://us-cert\[.\]cisa\[.\]gov/sites/default/files/publications/MAR-10292089-1.v1.stix.xml](https://us-cert[.]cisa[.]gov/sites/default/files/publications/MAR-10292089-1.v1.stix.xml)
- Additional information available at [https://us-cert\[.\]cisa\[.\]gov/china](https://us-cert[.]cisa[.]gov/china)





# TLP: WHITE - CISA Activity Alert AA20-209A - Potential Legacy Risk from Malware Targeting QNAP NAS Devices

- Joint alert from CISA and the UK NCSC summarizes findings from the CISA and NCSC investigation and analysis of a strain of QSnatch malware. Mitigation advice is also provided.
- The CISA advisory includes mitigation recommendations, and links to vendor-specific resources for affected products
- STIX IOCs available at [https://us-cert\[.\]cisa\[.\]gov/sites/default/files/publications/AA20-209A.stix.xml](https://us-cert[.]cisa[.]gov/sites/default/files/publications/AA20-209A.stix.xml)
- Full report available at:
  - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa20-209a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-209a)
  - [https://www\[.\]ncsc\[.\]gov\[.\]uk/files/NCSC%20CISA%20Alert%20-QNAP%20NAS%20Devices.pdf](https://www[.]ncsc[.]gov[.]uk/files/NCSC%20CISA%20Alert%20-QNAP%20NAS%20Devices.pdf)



# TLP: WHITE - CISA Activity Alert AA20-206A Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902

- Alert released in response to recently disclosed exploits that target F5 BIG-IP devices that are vulnerable to CVE-2020-5902
- Unpatched F5 BIG-IP devices are an attractive target for malicious actors. F5's security advisory for CVE-2020-5902 states that there is a high probability that any remaining unpatched devices are likely already compromised.
- AA20-206A includes technical details, detection methods, and mitigations for this vulnerability.
- Alert at <https://us-cert.cisa.gov/ncas/alerts/aa20-206a>
- F5 patch and detection tool at <https://support.f5.com/csp/article/K52145254>



# TLP: WHITE – AA20-205A – NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems

- Actions listed in AA20-205A are intended to ensure that critical asset owners and operators of critical infrastructure take immediate steps to ensure resilience and safety of U.S. systems should a time of crisis emerge in the near term.
- Recommendations are directed at all DoD, NSS, DIB, and U.S. critical infrastructure to take immediate actions to secure their operational technology (OT) assets.
- AA20-205A includes recently observed TTPs, impacts, and mitigation recommendations
- Available at [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa20-205a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-205a) and [https://media\[.\]defense\[.\]gov/2020/Jul/23/2002462846/-1/-1/1/OT\\_ADVISORY-DUAL-OFFICIAL-20200722.PDF](https://media[.]defense[.]gov/2020/Jul/23/2002462846/-1/-1/1/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF)



# TLP: WHITE – AA20-195A Critical Vulnerability in SAP NetWeaver AS Java

- SAP released a security update to address a critical vulnerability, CVE-2020-6287, affecting the SAP NetWeaver Application Server (AS) Java component LM Configuration Wizard.
- CISA strongly recommends organizations immediately apply patches, prioritizing internet-facing systems, followed by internal systems
- If patching cannot be done immediately, mitigation of the vulnerability can be done by disabling the LM Configuration Wizard service (see SAP Security Note #2939665 at [https://Launchpad\[.\]support\[.\]sap\[.\]com/#/notes/2939665](https://Launchpad[.]support[.]sap[.]com/#/notes/2939665))
- The activity alert is available at [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa20-195a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-195a)



# TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- CISA News Room - [https://www\[.\]cisa\[.\]gov/cisa/newsroom](https://www[.]cisa[.]gov/cisa/newsroom)
- CISA Publications Library - [https://www\[.\]cisa\[.\]gov/publications-library](https://www[.]cisa[.]gov/publications-library)
- CISA Cyber Resource Hub - [https://www\[.\]cisa\[.\]gov/cyber-resource-hub](https://www[.]cisa[.]gov/cyber-resource-hub)
- CISA Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) - [https://www\[.\]us-cert\[.\]gov/resources/ncats/](https://www[.]us-cert[.]gov/resources/ncats/)
- CISA Cybersecurity Directives - [https://cyber\[.\]dhs\[.\]gov/directives/](https://cyber[.]dhs[.]gov/directives/)
- CISA COVID-19 Response – [https://www\[.\]cisa\[.\]gov/coronavirus](https://www[.]cisa[.]gov/coronavirus)





For more information:  
[cisa.gov](https://www.cisa.gov)

Questions?  
[CISAServiceDesk@cisa.dhs.gov](mailto:CISAServiceDesk@cisa.dhs.gov)  
1-888-282-0870



# AUTO-ISAC COMMUNITY MEETING

## Why Do We Feature Speakers?

- ❖ These calls are an opportunity for information exchange & learning
- ❖ Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

## What Does it Mean to Be Featured?

- ❖ Perspectives across our ecosystem are shared from members, government, academia, researchers, industry, associations and others.
- ❖ Goal is to showcase a rich & balanced variety of topics and viewpoints
- ❖ Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC

**30+**  
*Featured  
Speakers to  
date*

**7** *Best  
Practice  
Guides  
available on  
website*

**2000+**  
*Community  
Participants*

## How Can I Be Featured?

- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!



*Slides available on our website* – [www.automotiveisac.com](http://www.automotiveisac.com)





# FEATURED SPEAKER

## GARY BERMAN



# GARY BERMAN, CEO OF CYBERMAN SECURITY, LLC

## CREATOR, *THE CYBER HERO ADVENTURES: DEFENDERS OF THE DIGITAL UNIVERSE*



Gary is the Creator of The Cyber Hero Adventures: Defenders of the Digital Universe comic training series, Host of The Unsung Cyber Hero Adventures video podcast, Cybersecurity Reporter for Cyber Defense Magazine and CEO of Cyberman Security, LLC.

Gary refers to himself as the “Forrest Gump” of cybersecurity because, until the last several years, he knew very little about technology and even less about cyber security, but everything about the devastating effects of being the CEO of a company that was victimized by a persistent series of insider attacks and forced to close.

Gary has decided to pivot from being a victim to becoming an advocate to help keep others from suffering the life-altering consequences of being hacked. Like many of you, he has attended over 50 cybersecurity conferences to listen and learn and this year he was labeled an “Industry Analyst” by the Consumer Electronics Association. He has given speeches to many organizations including the DoD regarding their CMMC initiative.



## Auto-ISAC



*Gary Berman, Creator, "The CyberHero Adventures:  
Defenders of the Digital Universe"*

### Our Mission

The only time that people hear about hacks or cybersecurity is when the "Black Hats" win. "

Our mission is to support the Community and to say **THANK YOU** by shining the light on all of the unsung heroes who toil in anonymity to keep us safe while online at work, home and school".

## Today's Discussion



1. Humanizing Cybercrime: An Insider Threat Case Study
2. Meet the "Forrest Gump" of Cybersecurity
3. The BIG Pivot: From Victim to Advocate
4. The Future

# What the heck am I doing here?



## Defending YOUR Wheels & Your Health: Kevin Tierney, Vice President of Global Cybersecurity, General Motors

Jun 3rd, 2020 by unsunghero

Watch Now:



- 2 Interviews
- Global Scale Challenges
  - Vehicle Security
  - Supply Chain Security
- Electric Vehicles
- Self Driving Vehicles
- Team Members
  - Working from Home
  - Workplace & Covid-19
  - Diversity & Inclusion

# 1. A View from the C-Suite: An Insider Threat Case Study



- Company founded in 1988.
- 100+ Employees.
- Sold 49% to one of the largest marketing companies in the world.
- AT&T, Best Buy, Ford, General Motors, P&G etc. as clients.

## Daily Parking Lot Summits of Trusted Employees



Called biggest clients alleging fraud.

Lost Millions.

- Near-death injury.
- Small group of employees started their OWN company while working for us full-time.
- Duplicated website
- Redirected calls
- Stole intellectual property

We lost everything...and so did all of our employees.

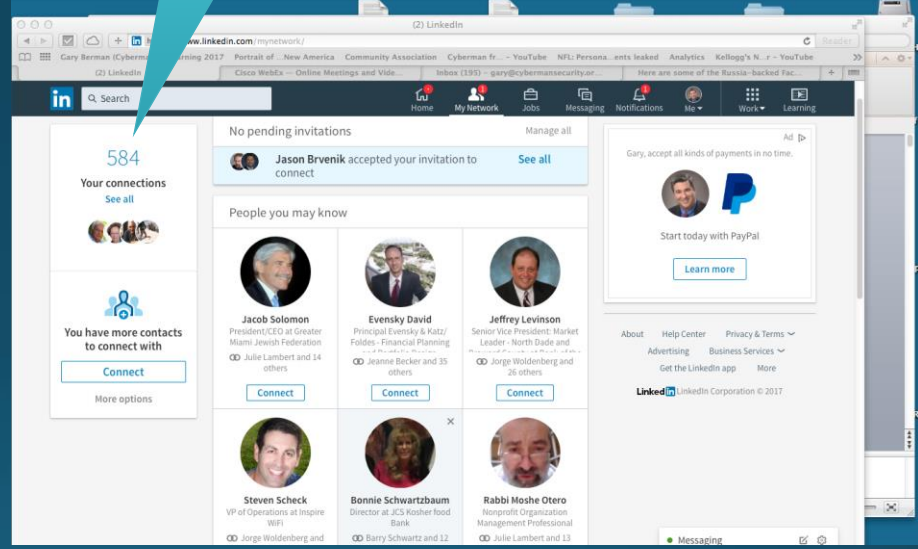
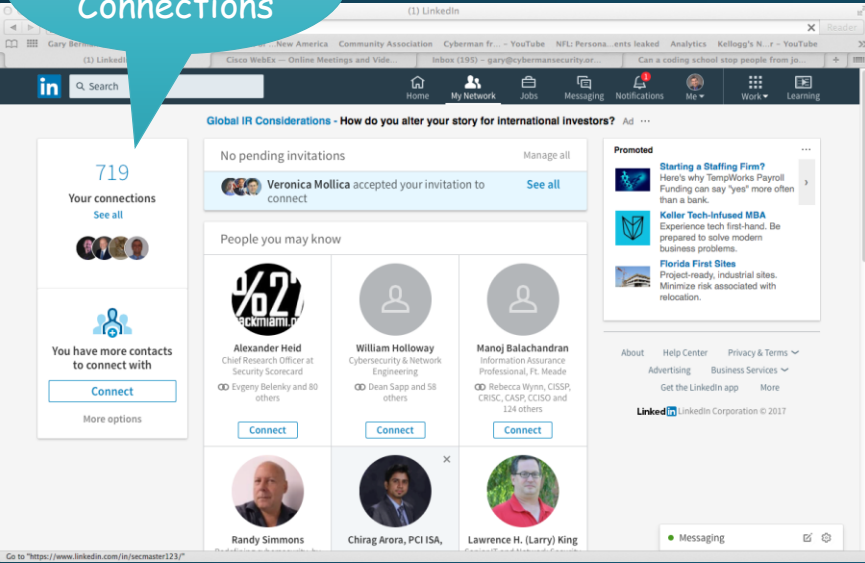




# LinkedIn Spoof

719  
Connections

LinkedIn "2"  
584  
Connections



# Cybersecurity Experts

I could not afford a complete analysis, 90% chance of Man in the Middle Attack

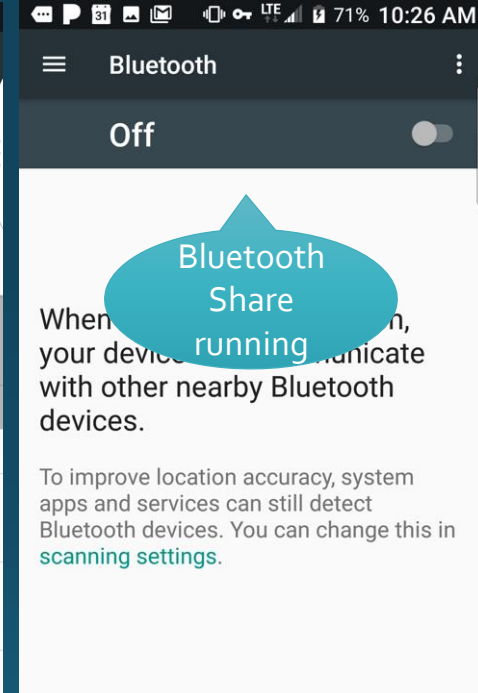
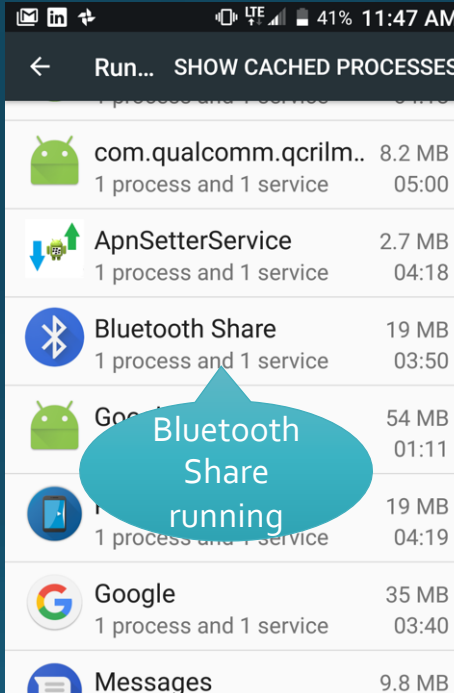
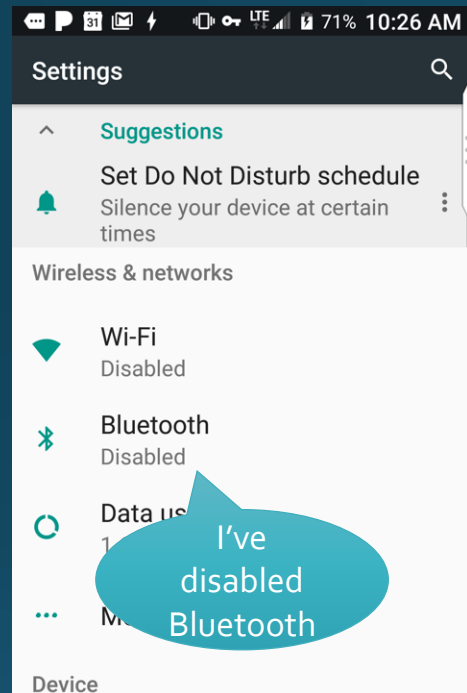
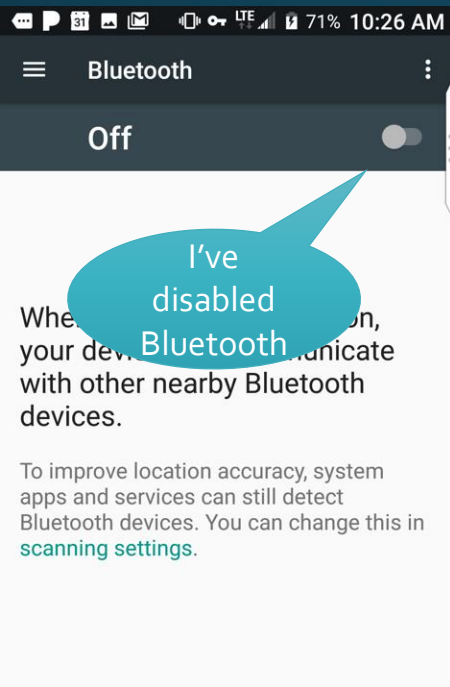
## Client Security Report

Gary Berman

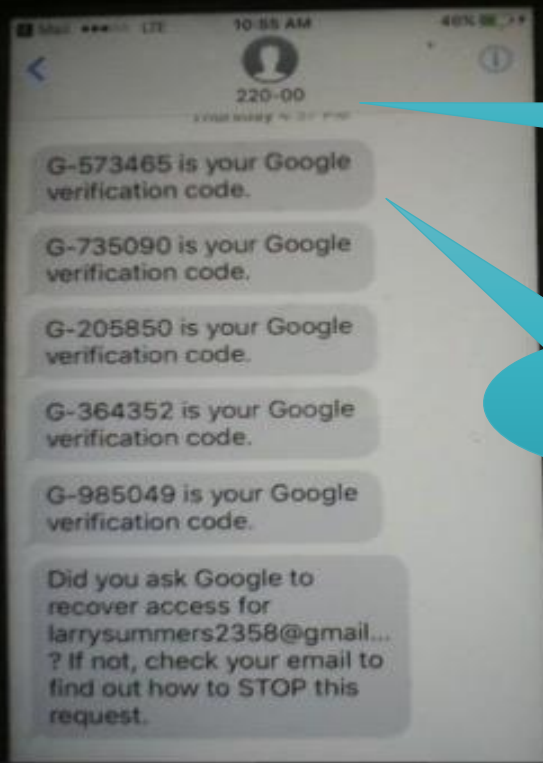
### Conclusion:

The log files were deleted before 09/15. The laptop was compromised through the one of the multiple vulnerabilities with a probability 90%. The list of vulnerability of that OS version includes OpenSSH (the remote access to console) and mitm or network intrusion with privilege escalation. Hacker can gain access remotely with high privileges and destroying all the signs of their deeds. Such as the destroying logs that were before 09/15.

# Worked non-stop to gather photographic evidence. 19 Attack Vectors



# Google 2-Step Verification was Spoofed on iPhone

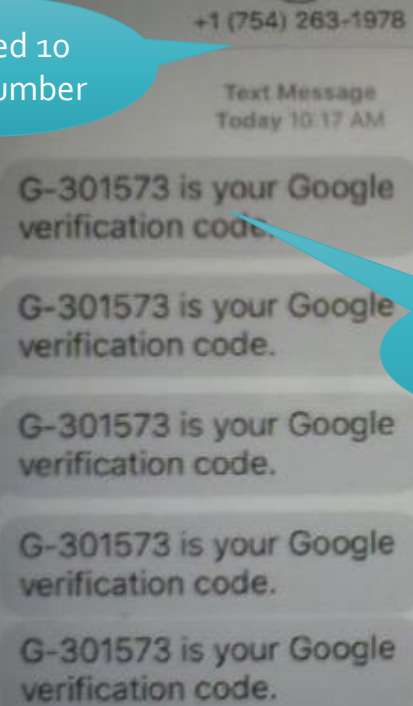


Masked 5 Digit Number

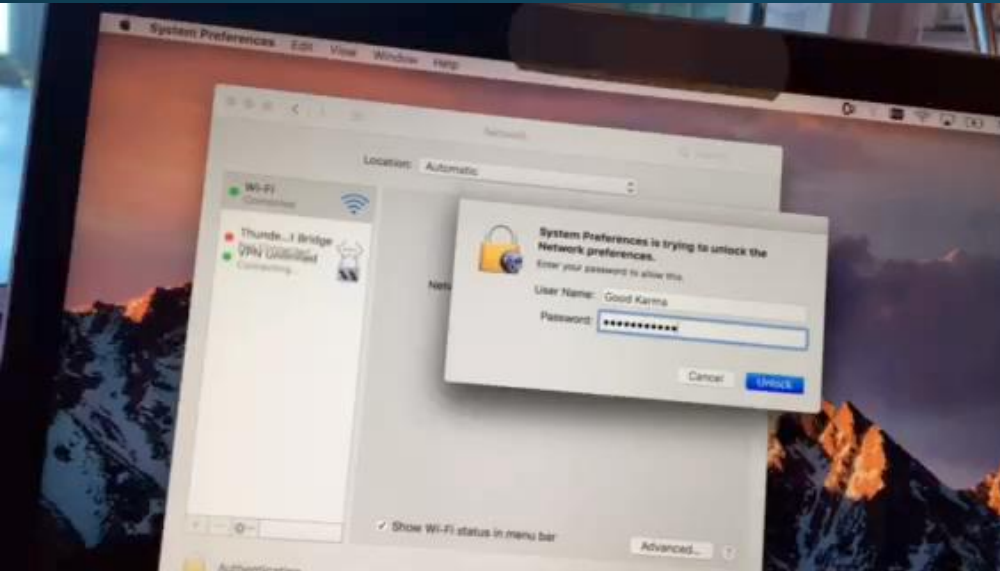
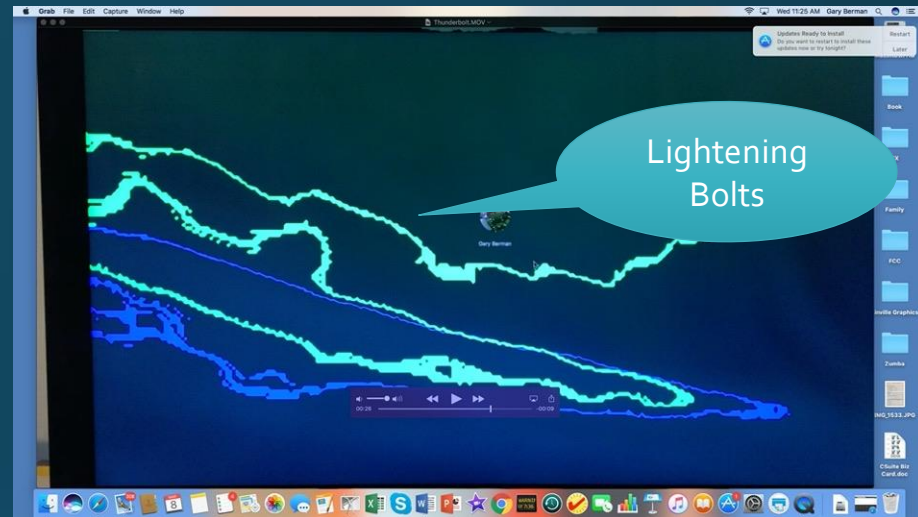
Correct Single Use Unique Codes

Spoofed 10 Digit Number

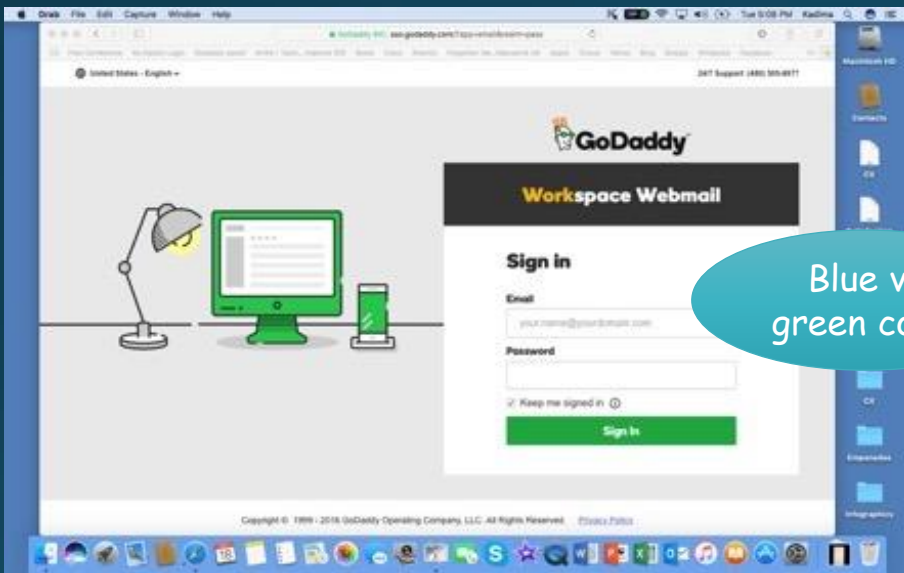
Same Number Every Time



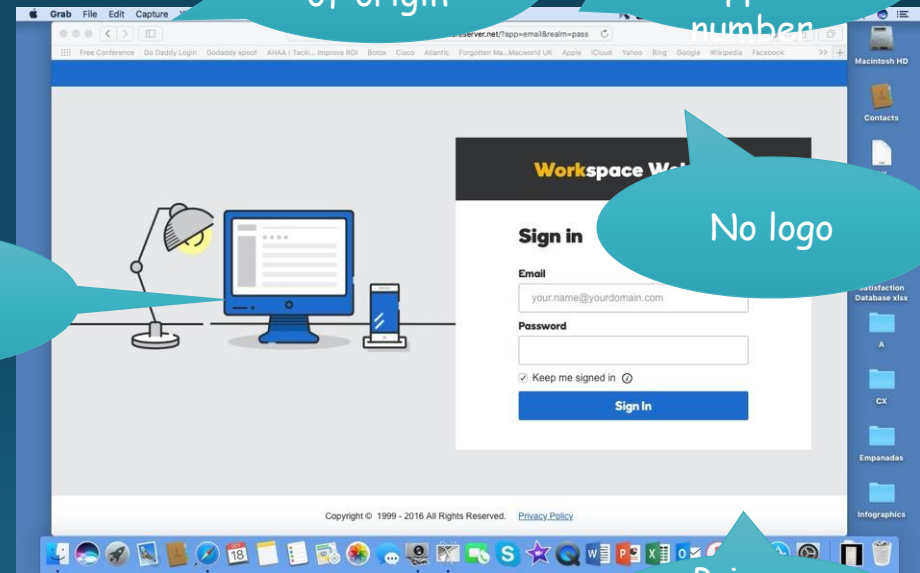
Thunderstrike signature  
to indicate that hack has begun



# Multiple E-mail Systems Compromised



Blue vs  
green color



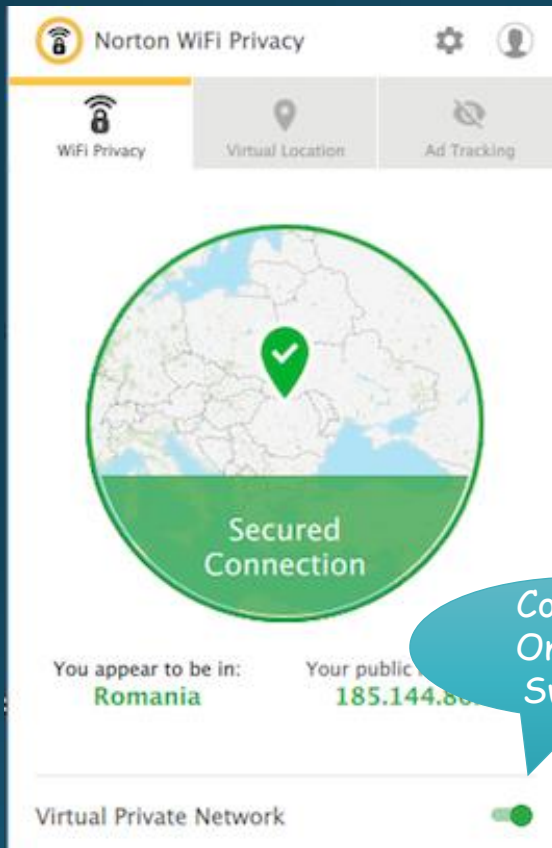
No country  
of origin

No  
customer  
support  
number

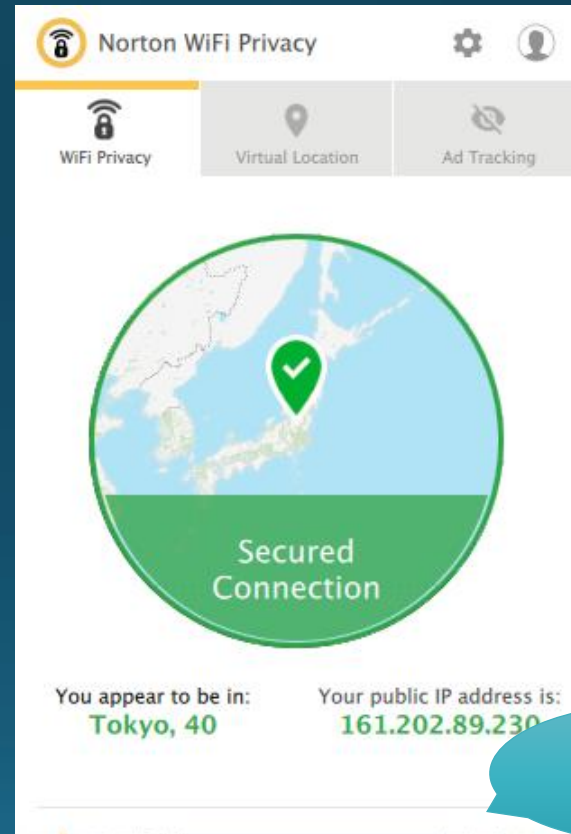
No logo

Privacy  
policy error  
message

# Norton VPN Spoof.



Correct  
On/Off  
Switch

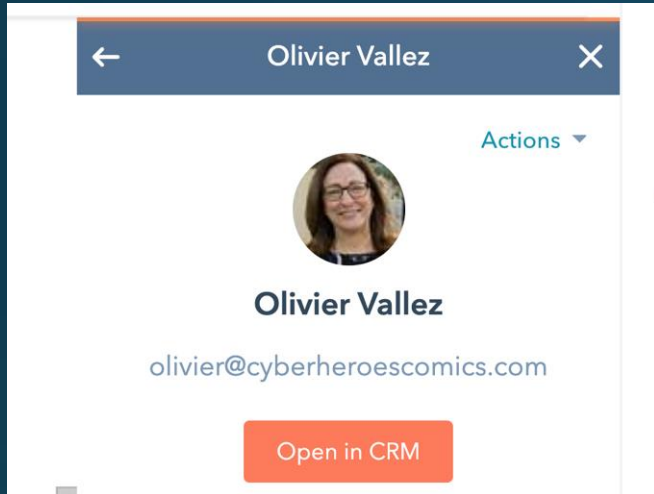


No VPN  
On/Off  
Switch






# At least the hacker had a sense of humor...



← Olivier Vallez ×

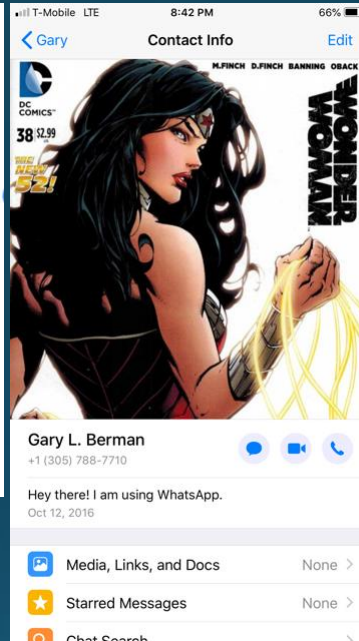
Actions ▾



**Olivier Vallez**


olivier@cyberheroescomics.com

Open in CRM



⋮ T-Mobile LTE 8:42 PM 66%

← Gary Contact Info Edit



DC COMICS™  
38 \$2.99

MY MOM, MYSELF  
WONDER WOMAN REBORN

**Gary L. Berman**

+1 (305) 788-7710

Hey there! I am using WhatsApp.

Oct 12, 2016

- Media, Links, and Docs None >
- Starred Messages None >
- Chat Search >



From gary.berman@cyberdefensemagazine.com

To **OV** Olivier Vallez ×

Bcc

Great. This will be. a. win-win. Look at the. extra periods. Church Lady:)

Thanks!

Gary Berman  
Cybersecurity Reporter  
[Cyber Defense Magazine](#)  
786-858-2632  
gary.berman@cyberdefensemagazine.com

Random Punctuations

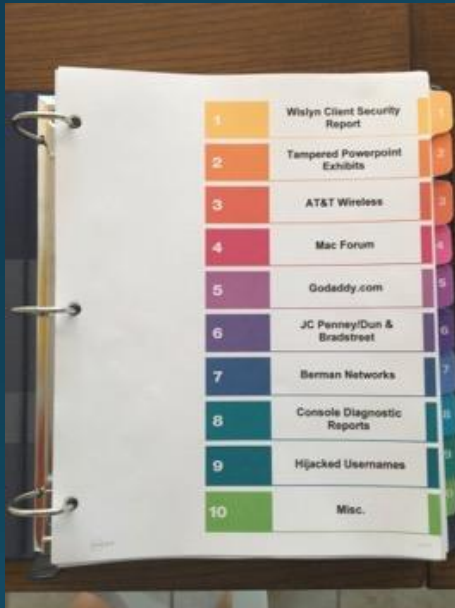


# 57 Potential Consequences of an Insider Attack as per Carnegie Mellon's Insider Threat Report



- Physical/Digital
- Economic
- Psychological
- Reputational
- Social/Societal

## Law Enforcement

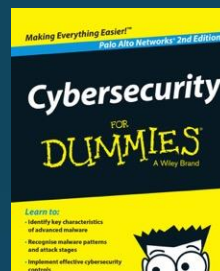


- Local Police Department (5 times).
- FBI (4 times).
- Secret Service (2 times).
- District Attorney declined to open case due to lack of evidence/attribution.

“Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman”.

Justice Louis D. Brandeis

## 2. Meet the "Forrest Gump" of Cyber Security

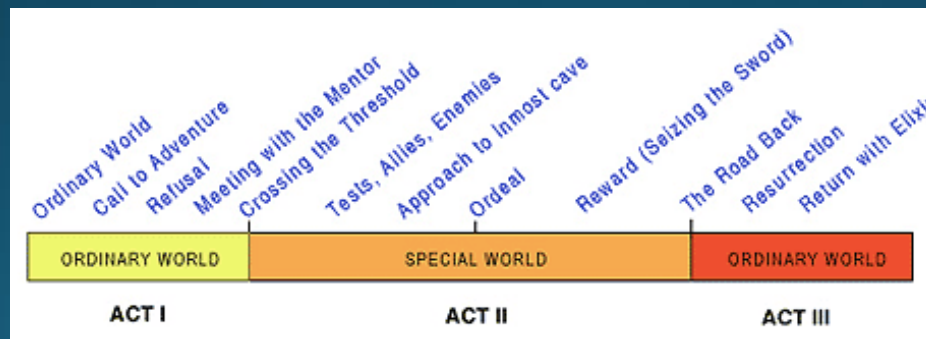




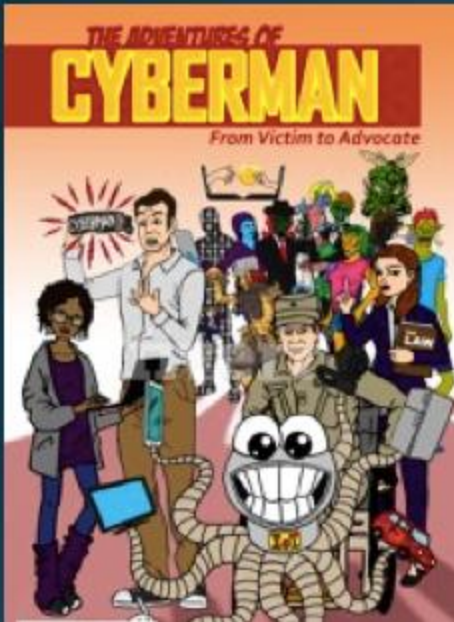
### 3. The BIG Pivot: From Victim to Advocate.



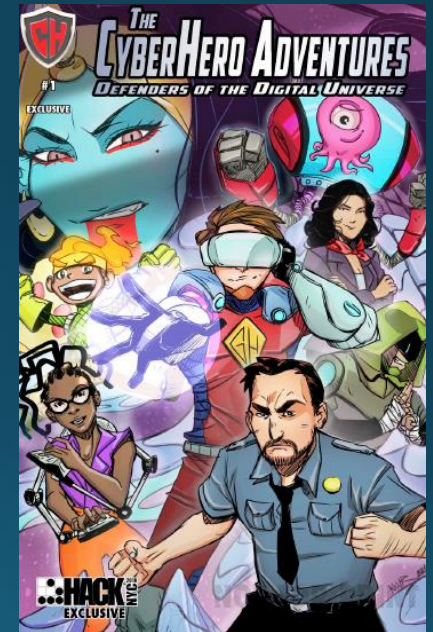
Joseph Campbell "The Heroes Journey"



## THANK YOU Stan Lee: "The Marvel Way"



- Blend continuity with renewal
- Sphere | Cube | Cylinder
- 6 heads high vs 8.5
- Passive vs action
- Average vs heroic
- Bland vs passionate
- Vertical vs forward perspective





# Meet the Cyber Heroes: Real-Life Unsung Heroes!



=



People LOVE to share their FUN!



Our FIRST solo flight!



# The CyberHero Adventures: Defenders of the Digital Universe



# Meet the CyberHeroes!



LARRY JONES (A.K.A. CYBER HERO) KNEW THAT HE NEEDED HELP TO LEARN ABOUT TECHNOLOGY AND HACKING. THE MOST IMPORTANT THING THAT HE NEEDED TO UNDERSTAND WAS: WHY DO HACKERS DO WHAT THEY DO? AFTER LISTENING AND LEARNING ABOUT HACKING AND CYBER SECURITY FROM THE AMAZING PEOPLE IN LAW ENFORCEMENT, SUCH AS THE FBI, CYBER SECURITY EXPERTS, THE DEPARTMENT OF DEFENSE, THE DEPARTMENT OF HOMELAND SECURITY AND ACADEMIA, LARRY BEGAN TO UNDERSTAND THAT ALMOST ALL OF THE HACKERS WERE ACTUALLY TRYING TO HELP (WHITE HATS) BY DEFENDING THE WORLD AGAINST CYBER CRIMINALS (BLACK HATS).

THERE WERE ALSO MANY GREAT PEOPLE WHO WERE THREAT RESEARCHERS WHO DISCOVERED VULNERABILITIES IN COMPUTERS AND CONNECTED DEVICES TO HELP PROTECT US ALL (GREY HATS). LARRY KEPT HEARING THE NAME OF ONE PERSON WHO WAS CONSISTENTLY MENTIONED AS BEING THE BEST HACKER IN THE UNIVERSE: QUEEN JIO. FROM THE MOMENT THAT SHE WAS BORN, HER PARENTS KNEW THAT SHE WAS DESTINED TO BECOME A POWERFUL LEADER AND ROLE MODEL AND TO SHED SUNLIGHT ON A DARK WORLD, SO THEY NAMED HER JIO (AN ANCIENT TERM FOR "SUN"). HER FIRST WORDS WERE: WHO, WHAT, WHERE, WHEN AND MOST IMPORTANTLY...HOW? SHE QUICKLY DISCOVERED COMPUTERS AND PROGRAMMING AND HER DESTINY WAS SEALED TO SPREAD SUNSHINE ON A DIVERSE AND INCLUSIVE WORLD.

## QUEEN JIO™



LARRY IS A "BODILY OUI" WHO TOOK EMPLOYMENT AT MANAGING COMMUNICATIONS AND COOPERATE THERMODYNAMICS. HE RAN A SUCCESSFUL COMPANY THAT WAS SUBSEQUENTLY SOLD TO GLOBALCOM. EVERYTHING WAS GOING GREAT UNTIL ONE DAY HE RECEIVED A TALENTED CALL. UNEXPECTEDLY TO HIM, ONE OF LARRY'S EMPLOYEES NAMED GLOBALCOM BELONGING TO BE A WHISTLE-BLOWER AND SPREAD A SCANDAL THAT THERE WAS BENEVOLENT TRADING THROUGHOUT LARRY'S COMPANY AND THAT ALL CLIENTS SHOULD STOP ALL COMMUNICATIONS!

LARRY LOST MILLIONS OF DOLLARS AND HIS HOME. HE WAS FORCED TO FIRE ONE HUNDRED EMPLOYEES. ONLY THIRTEEN LEFT, LIKE PERKINS THE LATTER OF AN ONION. LARRY BEGAN TO UNDERSTAND THAT HE WAS BEING VICTIMIZED BY A SERIES OF INEPT CYBER ATTACKS THAT FUNELED HIS BUSINESS INTO A SHADOW COMPANY CONTROLLED BY SEVERAL FORMER EXECUTIVES. THEY IGNORED HIS WARNINGS, RE-EMERGED CALLS TO THE SHADOW COMPANY AND DESTROYED HIS REPUTATION. UNABLE TO PROVE HIS CASE AND SUFFERING WOUNDS DUE TO THE DIFFICULTY OF IDENTIFYING THE PLOT AND THE HACKER, LARRY DECIDED TO PIVOT FROM BEING A VICTIM TO BECOMING AN ADVOCATE. HE LEARNED EVERYTHING HE COULD ABOUT CYBER SECURITY. LIKE DOROTHY IN THE WIZARD OF OZ, LARRY MEETS WISE-DEEDFUL CYBERHEROES ALONG THE WAY, WHO ARE MISSION-DRIVEN CHARACTERS JOINING HIM ON HIS QUEST TO BRING AWARENESS OF CYBERCRIME AND TO DEFEND THE DIGITAL UNIVERSE!

## LARRY JONES & THE CYBERHERO!



WHILE ON TOUR OF THE FACILITY, LARRY AND SUPER AGENT K MEET TARA BIGHT, WHO WORKS AT THE INSTITUTE. THEY ARE INSTANTLY IMPRESSED WITH HER PASSION, KNOWLEDGE AND SKILLS AS A PROGRAMMER.

TARA CAME FROM HUMBLE BEGINNINGS. AGAINST ALL ODDS, AND WITH THE HELP OF EXPERT MENTORS IN THE TECHNOLOGY AND CYBERSECURITY FIELDS, SHE PROVED TO BE A LIGHTNING-FAST CODER.

SHE HAS DEDICATED HER CAREER TO OPENING UP THE WORLD OF CODING TO CHILDREN AND TO IMBUE A LOVE OF TECHNOLOGY IN THEM. TARA IS THE "PIED PIPER" OF PROGRAMMERS. HER MAIN MOTIVATION IS TO SHATTER THE GLASS CEILING FOR DIVERSITY IN TECHNOLOGY.

TO DEFEAT A HACKER, YOU NEED A BETTER HACKER! AND THE CYBERHEROES HAVE TWO OF THE VERY BEST!

## TARA BIGHT & THE SUPERCODER

# Meet the CyberHeroes!



JUSTINA IS A FIRST-GENERATION AMERICAN OF MEXICAN HERITAGE. FROM A YOUNG AGE, SHE DEFENDED THE DEFENSELESS. SINCE THEN, SHE ALWAYS KNEW SHE WOULD BE A LAWYER.

SHE SET OUT TO LEARN ALL SHE COULD ABOUT THE JUDICIAL SYSTEM. MANY YEARS LATER SHE BECAME A PUBLIC DEFENDER, DEFENDING THE RIGHTS OF THE ACCUSED. ONE DAY, SOMETHING SHOCKING HAPPENED TO JUSTINA AND HER COLLEAGUES, WHEN SHE CLICKED ON AN EMAIL AND ALL THE COMPUTERS IN THE OFFICE FROZE.

SHE LATER LEARNED HER OFFICE WAS BEING HELD FOR RANSOM. THEY HAD TO DECIDE: SHOULD THEY PAY? OR SHOULD THEY FIGHT?

JUSTINA THOUGHT: HARD. EVENTUALLY, SHE EVEN IDENTIFIED THE HACKER... OR SO SHE THOUGHT. WORKING WITH LAW ENFORCEMENT, SHE REALIZED THAT THE LEGAL SYSTEM HAD NOT KEPT PACE WITH THE CHANGING WORLD OF TECHNOLOGY. IN THE MEAN TIME, JUSTINA WAS UNABLE TO BRING THE CRIMINAL TO JUSTICE.

WHEN THE CYBER HEROES SHARED THEIR STORIES, SHE INSTANTLY TOLD THEM:

**"I'M IN!"**

**JUSTINA JASCO**  
**THE DEFENDER**



LEONIDAS SERVED HIS COUNTRY WITH DISTINCTION AS AN OFFICER IN THE MILITARY. HE AND HIS FAMILY HAVE MADE COUNTLESS SACRIFICES IN SERVICE TO AMERICA.

UNFORTUNATELY, DURING A PARTICULARLY VIOLENT BATTLE WITH THE ENEMY, LEONIDAS WAS SEVERELY WOUNDED AND CONFINED TO A WHEELCHAIR FOR THE REST OF HIS LIFE.

LEONIDAS HAS SUCH A POWERFUL LOVE FOR HIS COUNTRY THAT, EVEN AFTER HIS INJURIES, HE STILL WANTED TO SERVE. HE DECIDED HE WOULD EXPAND HIS MIND AND MOVE INTO MILITARY INTELLIGENCE. HIS MISSION: TO LISTEN AND LEARN ABOUT ATTACK VECTORS TARGETING THE UNITED STATES.

ONE PARTICULAR VECTOR THAT HE REALIZED IS INCREDIBLY DANGEROUS IS CYBER WARFARE. LEONIDAS RECEIVED IN-DEPTH TRAINING AND EARNED CERTIFICATIONS THAT DEVELOPED HIS SKILLS TO IDENTIFY THE ENEMY IN CYBERSPACE. AFTER HEARING LARRY'S AND SUPER AGENT K'S STORIES, LEONIDAS FINALLY FOUND THE TEAM TO HELP HIM ACCOMPLISH HIS MISSION.

**LEONIDAS**  
**THE CYBERSOLDIER**



SHE IS ALWAYS READY TO INFORM USING HER METICULOUSLY RESEARCHED POWER PRESENTATION SLIDES THAT PROJECT FROM A LENS IN HER COSTUME. SHE SUBDUES HER ADVERSARIES WITH SLIDES SO DENSE WITH DATA THAT THEY ARE OVERCOME BY INSTANT SLUMBER!

THE PRESENTER IS A SKILLED WASTE-HAT EX-HACKER, WHO NOW SPENDS HER TIME PROMOTING CYBERSECURITY EDUCATION AND FACILITATING PARTNERSHIPS BETWEEN GOVERNMENT, ACADEMIA, AND THE PRIVATE SECTOR FOCUSED ON SUPPORTING PEOPLE'S ABILITY TO ADDRESS CURRENT AND FUTURE CYBERSECURITY ISSUES AND WORKFORCE CHALLENGES THROUGH STANDARDS AND BEST PRACTICES.

EVEN HER JOB DESCRIPTION PUTS YOU TO SLEEP!

**THE PRESENTER**

# Say "Boo" to the Villains!



HALF HUMAN, HALF INSECT, **BORIS** IS ABLE TO DETECT AND EXPLOIT VULNERABILITIES IN TECH DEVICES TO GAIN UNAUTHORIZED ACCESS PRIVILEGES, COMPROMISE DATA CONFIDENTIALITY AND INTEGRITY, AND WREAK HAVOC ON EVERYTHING HE TOUCHES.

**BORIS** HAS BEEN CREATING CHAOS FOR A LONG TIME. FOR EXAMPLE, IN 1996, A SOFTWARE BUG IN ITS GUIDANCE COMPUTER SOFTWARE FORCED THE EUROPEAN SPACE AGENCY TO DESTROY A \$1 BILLION ARIANE 5 PROTOTYPE ROCKET LESS THAN A MINUTE AFTER LAUNCH.

## BORIS THE BUGGER



WANNACRY IS AN INSIDIOUS FORM OF MALICIOUS CRYPTOMALWARE THAT ATTACKED THE MICROSOFT WINDOWS OPERATING SYSTEMS OF INDIVIDUALS AND BUSINESSES AROUND THE WORLD BY INJECTING THE USER'S DATA (LOCKING THEM OUT OF THEIR COMPUTER) AND DEMANDING RANSOM. IN SPECIAL PAYMENTS (TRACE DIGITAL CURRENCY) SUCH AS BITCOIN TO UNLOCK IT), MAKING PROGRAMMING AND EXECUTING THE REPARATIONS DIFFICULT. THE ATTACK WENT UNDISCOVERED IN SEVERAL INFECTED BODIES OVER 230,000 COMPANIES IN OVER 150 COUNTRIES.

WANNACRY ATTACKS ARE TYPICALLY CAUSED OUT USING A TROJAN HORSE DISGUISED AS A LEGITIMATE FILE. THE USER IS GUINED INTO DOWNLOADING OR OPENING IT IN AN EMAIL ATTACHMENT. HOWEVER, THE WANNACRY WORM WOULD BE HELD IN A DIMENSIONAL BETWEEN COMPUTERS WITHOUT ANY DATA INTERACTION.

THE ORIGINAL BODILY WANNACRY WAS STOLEN OUT IN THE UNITED STATES, DEVELOPING NEW TROJAN CODING NEW VARIANTS, FLOWING THESE

**INTERPOL**  
Case #  
F-349374E-780

**WILBUR WANNACRY**

**NEXT BIG ATTACK!**



THIS INFORMATION IS QUICKLY USED TO STEAL MONEY FROM ACCOUNTS AND TO APPLY FOR FRAUDULENT LOANS AND CREDIT CARDS. UNDOING THE DAMAGE CAUSED BY IDENTITY THEFT USUALLY TAKES MONTHS OF PHONE CALLS, WRITTEN COMMUNICATION, AND LOTS OF LEGAL AND FINANCIAL BUD TIME. KNOWING HOW TO SPOT THE SIGNS OF A PHISHING ATTACK (LOOKING AT THE SENDER'S ACTUAL EMAIL ADDRESS FOR EXAMPLE) CAN BE THE DIFFERENCE BETWEEN AN ONSET OF FRAUDULENCE AND THE SHARP PAIN OF OBTAINING THE SMALL AND BEING DONE WITH IT.

AS A GENERAL RULE, NO LEGITIMATE COMPANY WILL EVER ASK A CUSTOMER TO REVEAL SENSITIVE INFORMATION VIA EMAIL. WHEN IN DOUBT, INSTEAD OF CLICKING THE LINK PROVIDED IN THE EMAIL, TYPE THE COMPANY'S URL DIRECTLY INTO YOUR BROWSER OR CALL A COMPANY REPRESENTATIVE USING A KNOWN OR PUBLISHED PHONE NUMBER INSTEAD OF A PHONE NUMBER PROVIDED IN THE EMAIL.

THE **PHISHER** SENDS ITS PEST BY PRETEXTING TO BE A LEGITIMATE COMMUNICATION FROM A TRUSTED CONTACT (OF WHICH OFTEN THE "VICTIM IS A CUSTOMER) - OR - FROM THE HUNGRIER IDENTITY OF A FRIEND, COLLEAGUE, OR FAMILY MEMBER.

USING ONE OF MANY METHODS (USUALLY INVOLVING SOME "PROBLEMS" WITH THE ACCOUNT), THE PHISHER ENCOURAGES THE POTENTIAL VICTIM TO REVEAL SENSITIVE INFORMATION, SUCH AS LOG-IN IDS, PASSWORDS, PINs, SOCIAL SECURITY NUMBERS, ETC.

**F.B.I.**  
Case no.  
A-6455582  
Phoebe Phillips  
aka "The Phisher"

**PHOEBE THE PHISHER**

# Say "Boo" to the Villains!



FRAUDSTER, SCAMMER, CONFIDENCE ARTIST, GRIFTER, HUSTLER, CHAMELEON. HE GOES BY MANY NAMES. THEY ALL ADD UP TO ONE THING: SONNY THE SOCIAL ENGINEER IS A MASTER MANIPULATOR OF HUMAN BEHAVIOR. HIS GAME IS TO TRICK YOU INTO BELIEVING WHATEVER HE WANTS IN ORDER TO STEAL YOUR MOST VALUABLE AND PERSONAL INFORMATION.

HIS WEAPONS ARE BASED ON EMOTIONAL INTELLIGENCE. HE DOES NOT HESITATE TO TAKE ADVANTAGE OF THE MOST EXCITING OR SAD MOMENTS. HE WIELDS FEAR LIKE A WHIP. HE PREYS ON ANY PERCEIVED WEAKNESS TO BRING DOWN HIS TARGETS AND ENRICH HIMSELF IN THE PROCESS.

## SONNY THE SOCIAL ENGINEER



IVAN STEALS YOUR NAME, DATE OF BIRTH, SOCIAL SECURITY NUMBER, DRIVER'S LICENSE NUMBER, BANK ACCOUNT AND CREDIT CARD NUMBERS, PIN NUMBERS, ELECTRONIC SIGNATURES, PHOTOGRAPHS, AND INFORMATION... ALL IN AN EFFORT TO BECOME YOU!

BE ALERT FOR THE SIGNS OF STEALING YOUR MONEY AND REPUTATION FOR LOANS, CREDIT CARDS IN YOUR NAME!

- HAKING YOUR CREDIT CARDS THROUGH YOUR BANKING
- PURSUING YOUR PERSONAL DOCUMENTS AND PHOTOS
- SHIRKING YOUR CREDIT CARDS, CARS, AIRPORTS AND HOMES
- SEARCHING COMMON DATABASES SUCH AS "FIRST CAR TEST" OR "MOTOR VEHICLE REGISTRATION FROM CREDIT CARDS USING HAND-HELD CARD READERS"


IVAN ATTEMPTS TO ELICIT ACTIVITIES THROUGH YOUR "INTERESTS" OR OLD HUSB OR WIVES TO OBTAIN IDENTIFICATION INFORMATION

KNOWLEDGE: MOTHER'S MARRIAGE RECORDS OR NAME OR IDENTIFICATION FROM CREDIT CARDS USING HAND-HELD CARD READERS

"USING 'CONTACTLESS' CREDIT CARD READERS TO ACQUIRE DATA VULNERABILITY."

- DISCREETLY WATCHING OR LISTENING OTHER INDIVIDUALS' VALUABLE PERSONAL INFORMATION ("SHOULDER-SURFING")
- STEALING PERSONAL INFORMATION FROM COMPUTERS USING DEVICES IN BROWSER SECURITY FEATURES SUCH AS TOOLBAR KEYSTROKE LOGGING PROGRAMS
- HACKING COMPANIES TO OBTAIN LARGE QUANTITIES OF "BUILT-FORCE" WEBSITE
- BRIBING WEBSITE FOR PERSONAL DATA, OFFER IN ATTACKING WEAK PASSWORDS
- DIVERTING OR CREATING TOXIC AND CREDIT CARDS, BILLING STATEMENTS, OR NEW ACCOUNTS UNDER VICTIMS' NAMES

## IVAN THE IDENTITY THIEF



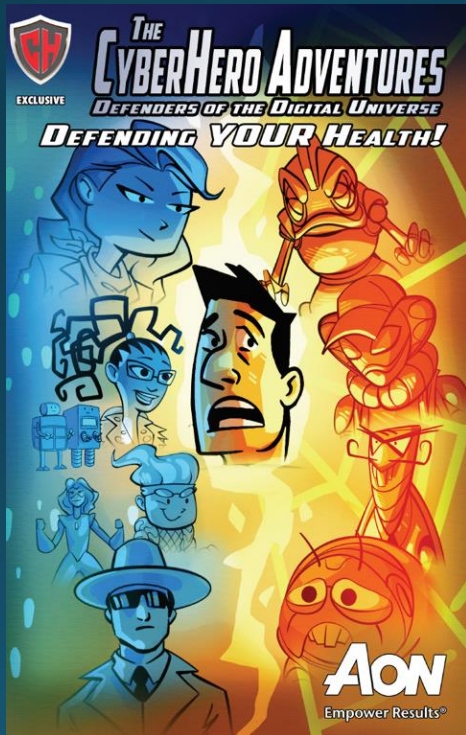
THE RAT IS AN INSIDIOUS CREATURE WHO IS VERY CLEVER AND STEALTHY. PAY NO ATTENTION TO HIS HORSE-LIKE BODY OR HIS Gnarly RAT FACE... BUT TO THE LENGTH OF HIS TAIL. IT'S SINEWY AND ABLE TO INSERT ITSELF, WITHOUT DETECTION, INTO ANY DEVICE ON THE INTERNET. MOST-COMMONLY IN PARTNERSHIP WITH THE PHISHER, A SIMPLE CLICK ON A LINK IN AN OFFICIAL-LOOKING EMAIL LETS THE RAT AND HIS CREW INTO YOUR LIFE TO TURN IT UPSIDE-DOWN. ONCE INSIDE, HE COMPLETELY TAKES CONTROL OF YOUR ONLINE EXISTENCE, WHICH HE CAN THEN MANIPULATE, DESTROY, AND DELETE.

## RANDALL R.A.T.

## 4. The Future

16 DHS Critical Infrastructure Sectors

Healthcare: "Defending YOUR Health"



Next Year? Defending YOUR Wheels



Virtual Reality Training





Thank YOU for being REAL-Life Cyber Heroes!

[www.cyberheroescomics.com](http://www.cyberheroescomics.com)

[gary@cyberheroescomics.com](mailto:gary@cyberheroescomics.com)



# OPEN DISCUSSION

*ANY QUESTIONS ABOUT THE  
AUTO-ISAC OR FUTURE TOPICS  
FOR DISCUSSION?*

# HOW TO GET INVOLVED: MEMBERSHIP

## IF YOU ARE AN OEM, SUPPLIER OR COMMERCIAL VEHICLE, CARRIER OR FLEET, PLEASE JOIN THE AUTO-ISAC!

- *REAL-TIME INTELLIGENCE SHARING*
- *INTELLIGENCE SUMMARIES*
- *REGULAR INTELLIGENCE MEETINGS*
- *CRISIS NOTIFICATIONS*
- *MEMBER CONTACT DIRECTORY*
- *DEVELOPMENT OF BEST PRACTICE GUIDES*
- *EXCHANGES AND WORKSHOPS*
- *TABLETOP EXERCISES*
- *WEBINARS AND PRESENTATIONS*
- *ANNUAL AUTO-ISAC SUMMIT EVENT*

*To learn more about Auto-ISAC Membership or Partnership, please contact Auto-ISAC! [contact.us@automotiveisac.com](mailto:contact.us@automotiveisac.com)*

# STRATEGIC PARTNERSHIP PROGRAMS

## Solutions Providers

*For-profit companies that sell connected vehicle cybersecurity products & services.*

*Examples: Hacker ONE, SANS, IOActive, GRIMM*

## Associations

*Industry associations and others who want to support and invest in the Auto-ISAC activities.*

*Examples: Alliance, ACEA, ATA, JAMA, CLEPA*

## Affiliations

*Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.*

*Examples: DHS, NHTSA, Colorado State, Johns Hopkins, NCI*

## Community

*Companies interested in engaging the automotive ecosystem and supporting the community.*

*Examples: Summit sponsorship – key events*

## INNOVATOR

### *Paid Partnership*

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed

## NAVIGATOR

### *Support Partnership*

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities

## COLLABORATOR

### *Coordination Partnership*

- “See something, say something”
- May not require a formal agreement
- Information exchanges- coordination activities

## BENEFACTOR

### *Sponsorship Partnership*

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

# AUTO-ISAC BENEFITS

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency



*Building Resiliency Across the Auto Industry*



# OUR CONTACT INFO

**Faye Francy**  
Executive Director



20 F Street NW, Suite 700  
Washington, DC 20001  
703-861-5417  
fayefrancy@automotiveisac.com

**Sharmila Khadka**  
Executive Organizational  
Secretary



20 F Street NW, Suite 700  
Washington, DC 20001  
sharmilakhadka@automotiveisac.  
com



[www.automotiveisac.com](http://www.automotiveisac.com)  
@auto-ISAC