HOSTED BY
Electrosoft
AND CAPITOL Technology University

TECHNOLOGY SUMMIT – 4rd IN THE SERIES

WELCOME

The Ransomware and Malware Conundrum

July 22, 2021 – 10AM – 12PM EDT

WELCOME / OPENING REMARKS

Dr. Bradford L. Sims
President
Capitol Technology University

Dr. Sarbari Gupta
CEO
Electrosoft Services, Inc.

Dr. Bradford L. Sims

PRESIDENT
Capitol Technology University

CAPITOL
Technology University

CAPITOL
Technology University

About Capitol Tech

Founded in 1927, and located in Laurel, Maryland, Capitol Tech is dedicated to education programs for professional opportunities in the evolving global community.

CAPITOL
Technology University

Nonprofit, Private, Accredited

Capitol is a nonprofit, private accredited university located in Laurel, Maryland, USA

CHE MSA
MIDDLE STATES COMMISSION ON HIGHER EDUCATION

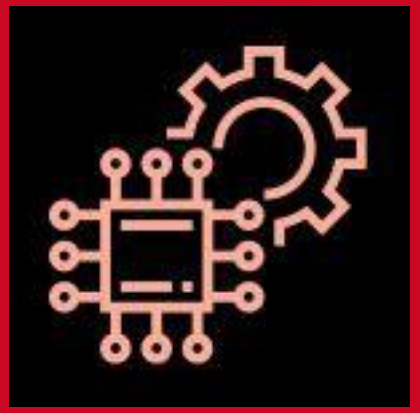
Capitol Technology University is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools.

MHEC
MARYLAND HIGHER EDUCATION COMMISSION

The University is authorized by the State of Maryland to confer Associate's (A.A.S.), Bachelor's (B.S.), Master's (M.S., M.B.A., T.M.B.A), and Doctoral (D.Sc., Ph.D.) degrees.

CAPITOL Technology University

Outstanding ROI



A Capitol Technology Degree is an outstanding investment in your future

Of the 4,500 Colleges & Universities in the U.S., Capitol is ranked

213th with a **20**-year NPV*

141st after **30** years

120th over a **40**-year work lifetime

(Georgetown University report)

*Net Present Value

CAPITOL Technology University

Award-Winning University

2020 Winner of the prestigious SC Media Award for

"Best Cybersecurity Higher Education Program"

2021 Finalist

Dr. William Butler, Chairperson Cybersecurity

2021 Winner of SC Media Award for

"Outstanding Educator"

National Center of Academic Excellence (CAE)
Northeast Regional Hub

ROYAL AERONAUTICAL SOCIETY

Aviation Programs Recognized by RAS

CAPITOL Technology University

Cyber Programs

Undergraduate

- BS Cybersecurity
- BS Cyber Analytics
- BS Management of Cyber and Information Technology
- BS Construction Information Technology and Cybersecurity

Masters

- MS Cybersecurity
- MRes Cyberpsychology
- MS Aviation Cybersecurity
- MS Construction Cybersecurity
- MS Cyber Analytics
- TMBA Business Administration and Cybersecurity

Doctoral Programs

- DSc Cybersecurity
- PhD Cyberpsychology
- PhD Cyber Leadership
- PhD Financial Cybersecurity
- PhD Healthcare Cybersecurity

Dr. Sarbari Gupta

CEO

Electrosoft Services, Inc.

Electrosoft

About Electrosoft

Electrosoft

www.electrosoft-inc.com

What We Do

- Deliver Technology Services & Solutions with Focus on Cybersecurity

Socio-Economic Status

- SBA 8(a) Program
- EDWOSB / WOSB

Competencies

- **Cybersecurity Compliance & Operations**
- **Identity, Credential & Access Mgmt.**
- **Program Management & IT Operations**
- **Software Solutions & Integration**
- **Enterprise IT Infrastructure Support**

About Electrosoft

Electrosoft

www.electrosoft-inc.com

Contract Vehicles

GSA Schedule
54151S; HACS; PIV

8(a) STARS II

OASIS
SB and 8(a) Pools 1 & 3

SeaPort-e

NITAAC
CIO-SP3

DLA JETS

eFAST
FAA eFAST

ITES-3S
Army ITES-3S

Who We Serve

1893 Metro Center Drive, Suite 228; Reston, VA 20190
P: 703-437-9451; E: info@electrsoft-inc.com

Hosted by Electrosoft and Capitol Technology University

The Ransomware and Malware Conundrum

- Any Organization can be a Target
- Role of Cyber Currencies and Cyber Insurance
- Defense Mechanisms
  - User Awareness and Training
  - Backup and Restoration
  - Border Control Techniques
  - Good Cyber Hygiene

Event Sponsor

Developer of **ThreatResponder**, an endpoint threat protection platform.

Pete Tseronis

Event Moderator

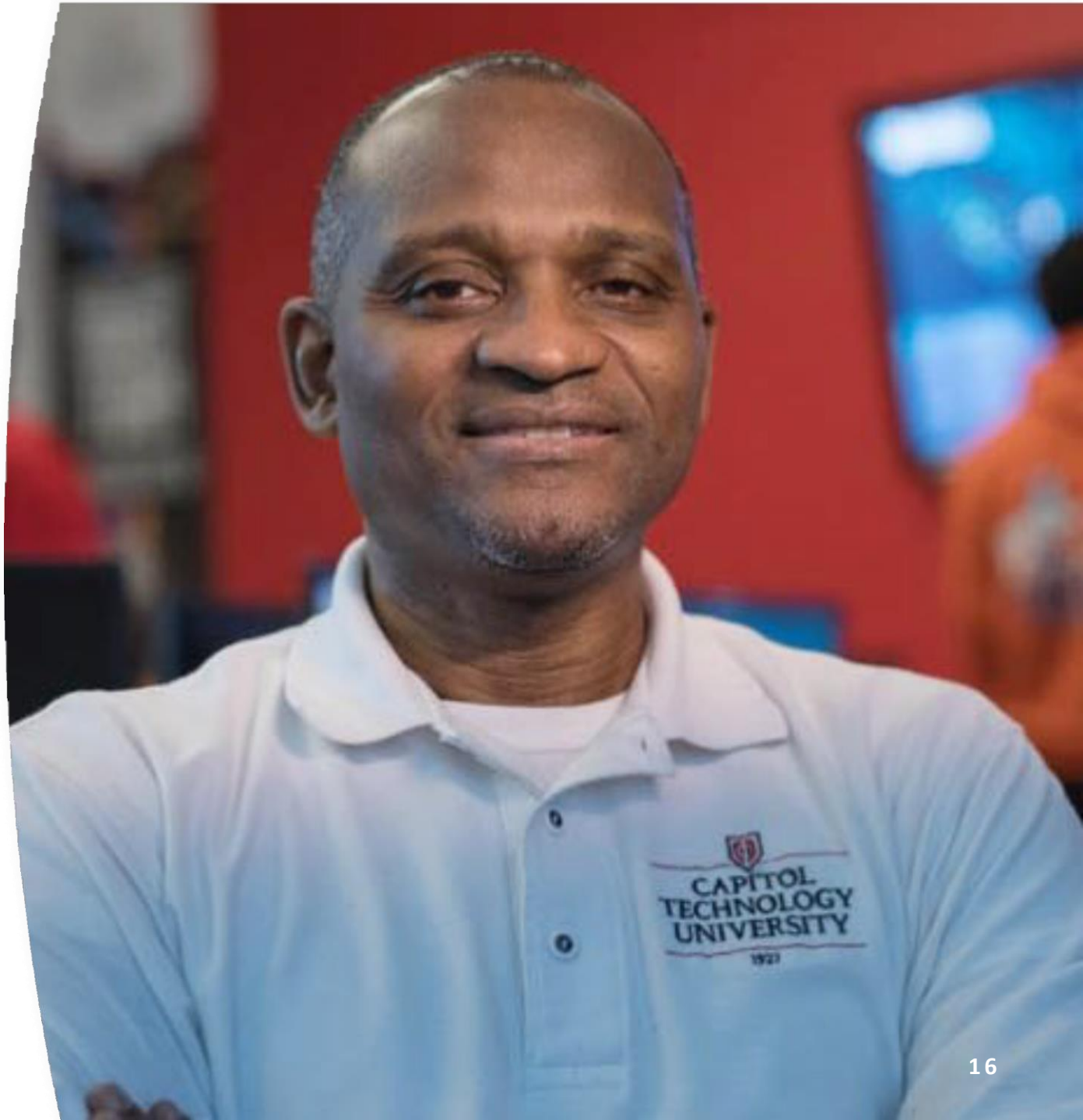
Founder & CEO -
Dots and Bridges LLC

Housekeeping Items

- Press Policy
- Questions
- Any Technical Challenges
- Brief Survey
- Recording available “on demand”

Opening Keynote Speaker

“The Ransomware Threat”



Dr. William Butler

Chair, Cyber and Information Security,
Director, Center for Cybersecurity Research and Analysis (CCRA)

Capitol Technology University

Agenda

- Malware / Ransomware
- Recent Malware Attacks
- Mitigation
- Threat Landscape
- What's ahead
- Federal Response
- Defensive Best Practices
- Role of AI/ML in Cybersecurity
- Collaboration
- Q & A

Malicious software (Malware)

Malware, short for "malicious software," includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data.

TYPES OF MALWARE

There are many unique types of malware that can infect your computer. Below is more information about a few of the more common types, according to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT

- **Adware:** a type of software that downloads or displays unwanted ads when a user online or redirects search requests to certain advertising websites.
- **Botnets:** networks of computers infected by malware and controlled remotely by cybercriminals, usually for financial gain or to launch attacks on websites or networks. Many botnets are designed to harvest data, such as passwords, Social Security numbers, credit card numbers, and other personal information.
- **Ransomware**: a type of malware that infects a computer and restricts access to it until a ransom is paid by the user to unlock it. Even when a victim pays the ransom amount, the stolen files could remain locked or be deleted by the cybercriminal.
- **Rootkit**: a type of malware that opens a permanent "back door" into a computer system. Once installed, a rootkit will allow additional viruses to infect a computer as various hackers find the vulnerable computer exposed and compromise it.
- **Spyware:** a type of malware that quietly gathers a user's sensitive information (including browsing and computing habits) and reports it to unauthorized third parties.
- **Trojan**: a type of malware that disguises itself as a normal file to trick a user into downloading it in order to gain unauthorized access to a computer.
- **Virus:** a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files entirely.
- **Worm**: a type of malware that replicates itself over and over within a computer.

https://www.cisa.gov/sites/default/files/publications/Malware_1.pdf/ransomware

Malware / Ransomware

Ransomware

Ransomware is a type of malicious software, or malware, that **prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.** Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

You can **unknowingly** download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with **malware**.

Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More menacing versions can **encrypt files and folders on local drives, attached drives, and even networked computers**.

Most of the time, you don't know your computer has been infected. You usually discover it when you can no longer access your data or you see computer messages letting you know about the attack and demanding ransom payments.

Revil demands $70 million to end biggest ransomware attack on record

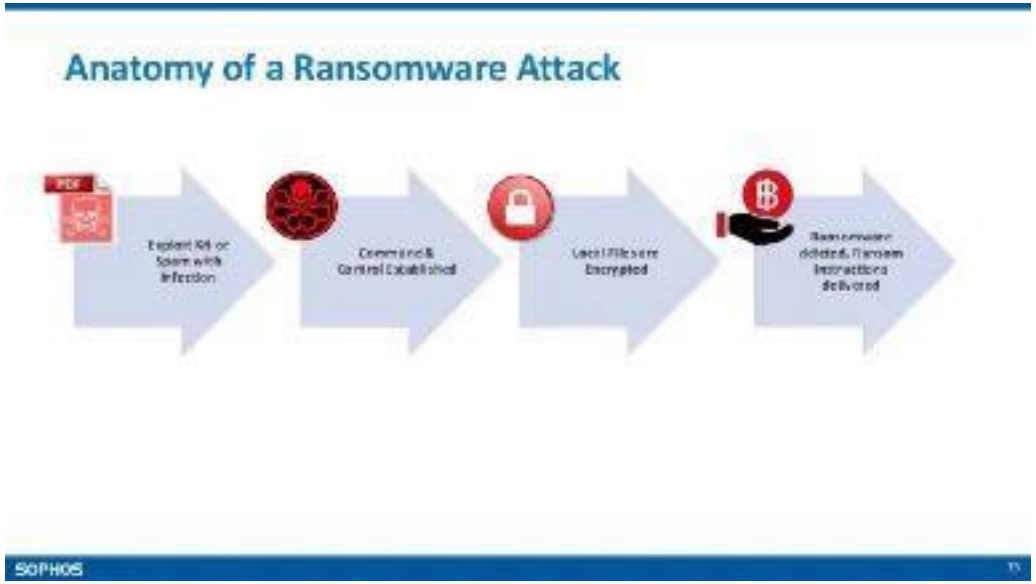
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

Recent Malware Attacks

- Solar Winds Dec 2020
- Microsoft Mar 2021
- MTA April 2021

  New York City Metropolitan Transportation Authority
- Colonial Pipeline May 2021 Paid 4.4 M
- JBS S.A. (Foods) May 2021 Paid 11 M

CNN



Ransomware gangs are getting more aggressive these days about pursuing payments and have begun stealing and threatening to leak sensitive documents if victims don't pay the requested ransom demand

- Leak sites are used to expose some stolen data
- Pressures companies to pay
- Sites are setup for victims to pay in bitcoin
- Encryption key is then sent

www.Zdnet.com

Mitigation

Tips for Avoiding Ransomware

The best way to avoid being exposed to ransomware—or any type of malware—is to be a **cautious and conscientious** computer user. Malware distributors have gotten increasingly savvy, and you need to be careful about what you download and click on.
Other tips:

•Keep operating systems, software, and applications current and up to date.

•Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans.

•Back up data regularly and double-check that those backups were completed.

•Secure your backups. Make sure they are not connected to the computers and networks they are backing up.

•Create a continuity plan in case your business or organization is the victim of a ransomware attack.

https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

How to Respond and Report

The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.

If you are a victim of ransomware:

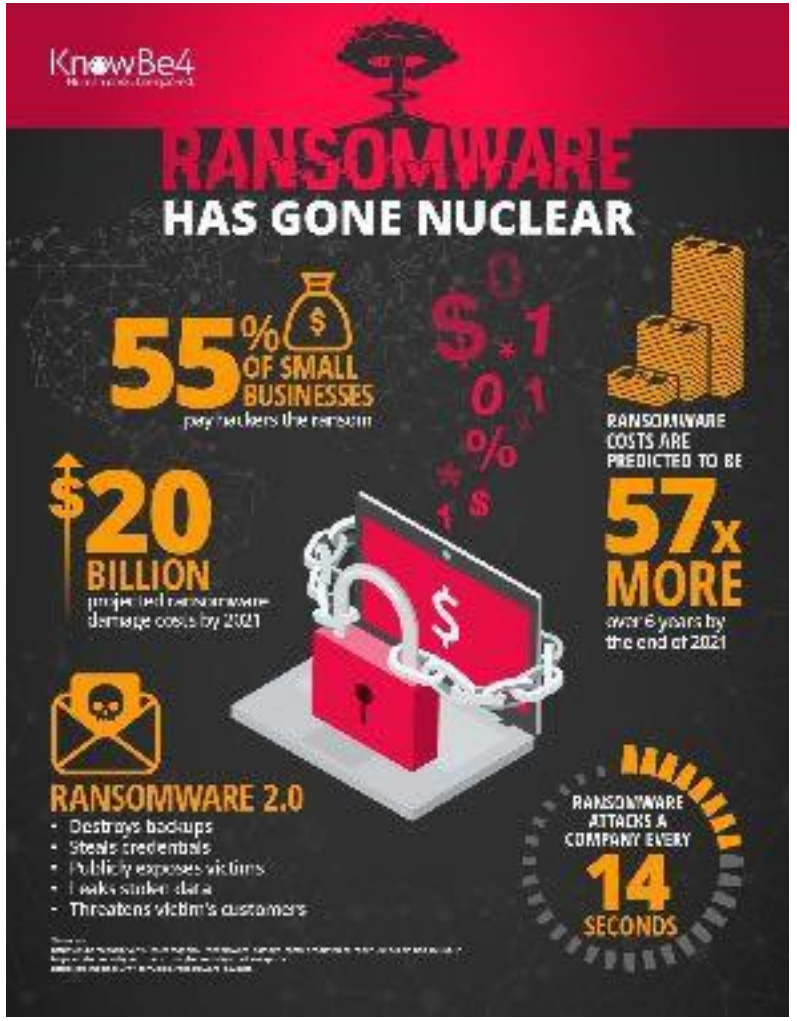
- Contact your local FBI field office to request assistance, or submit a tip online.
- File a report with the FBI's Internet Crime Complaint Center (IC3).

Threat Landscape

- Many ransomware groups operate globally, some under the direction or protection of their host nation
- Ransomware attacks increased by over 300% last year as companies switched to remote work
- Access brokers are threat actors that gain backend access to various organizations (both corporations and government entities) and sell this access either on criminal forums or through private channels.
- In 2020, hackers earned over $350 million
- Paying ransom encourages future attacks

Hacker Groups

- Revil,



https://news.youexec.com/briefs/us-government-launches-ransomware-task-force?r=news.&pt=wsd8syh3v2

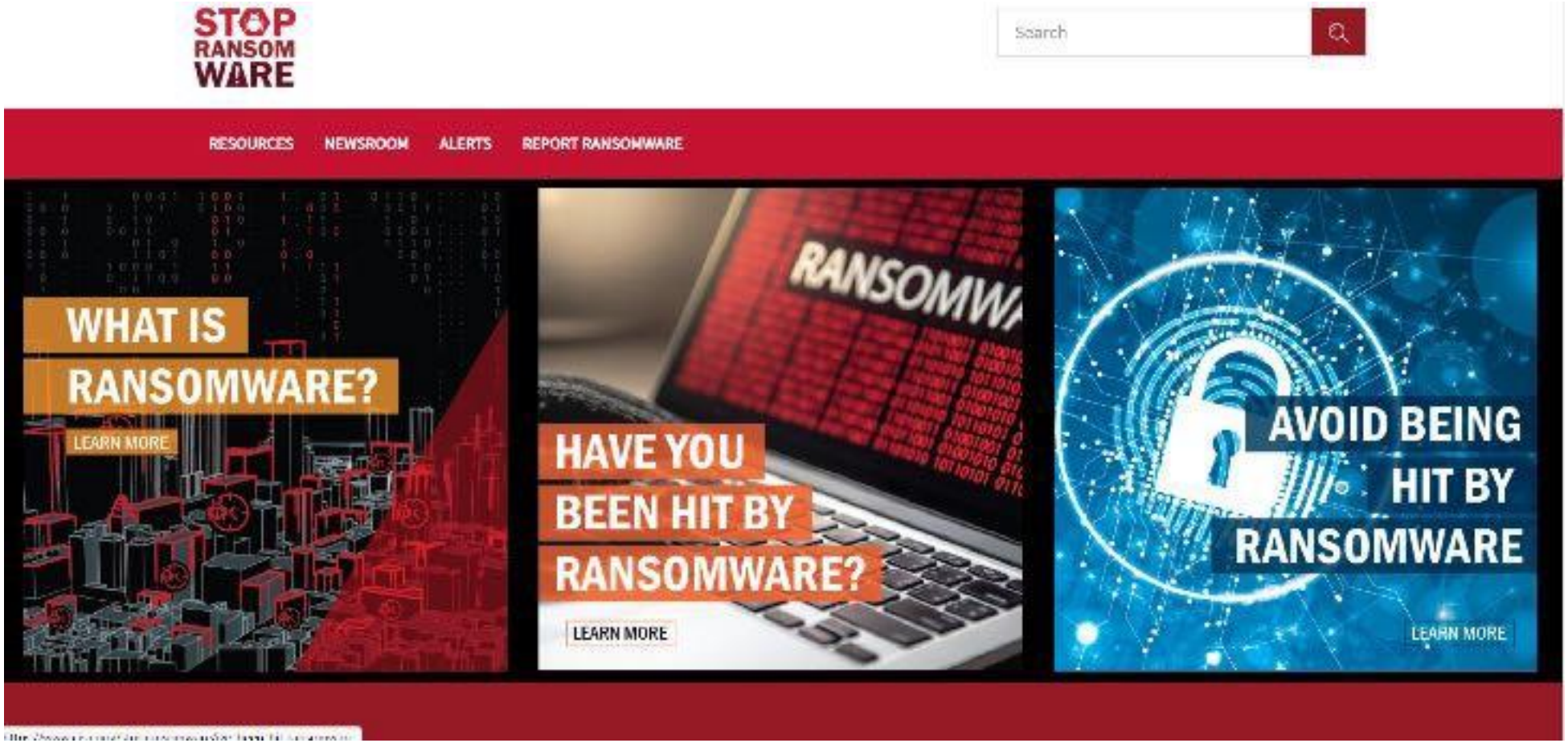
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

Federal Response

- President warns Putin to stop attacks on U.S. Critical Infrastructure from Russia
- Key senior cyber positions filled at White House and State Department
- The U.S. government will turn to the private sector for help to disrupt ransomware attacks as the world enters a perpetual "cyberwar"
- CISA also rolled out the "Reduce the Risk of Ransomware" Campaign in January
- White House forms Ransomware Task Force:
  - $10 million for information that identifies the hackers using their expertise for evil

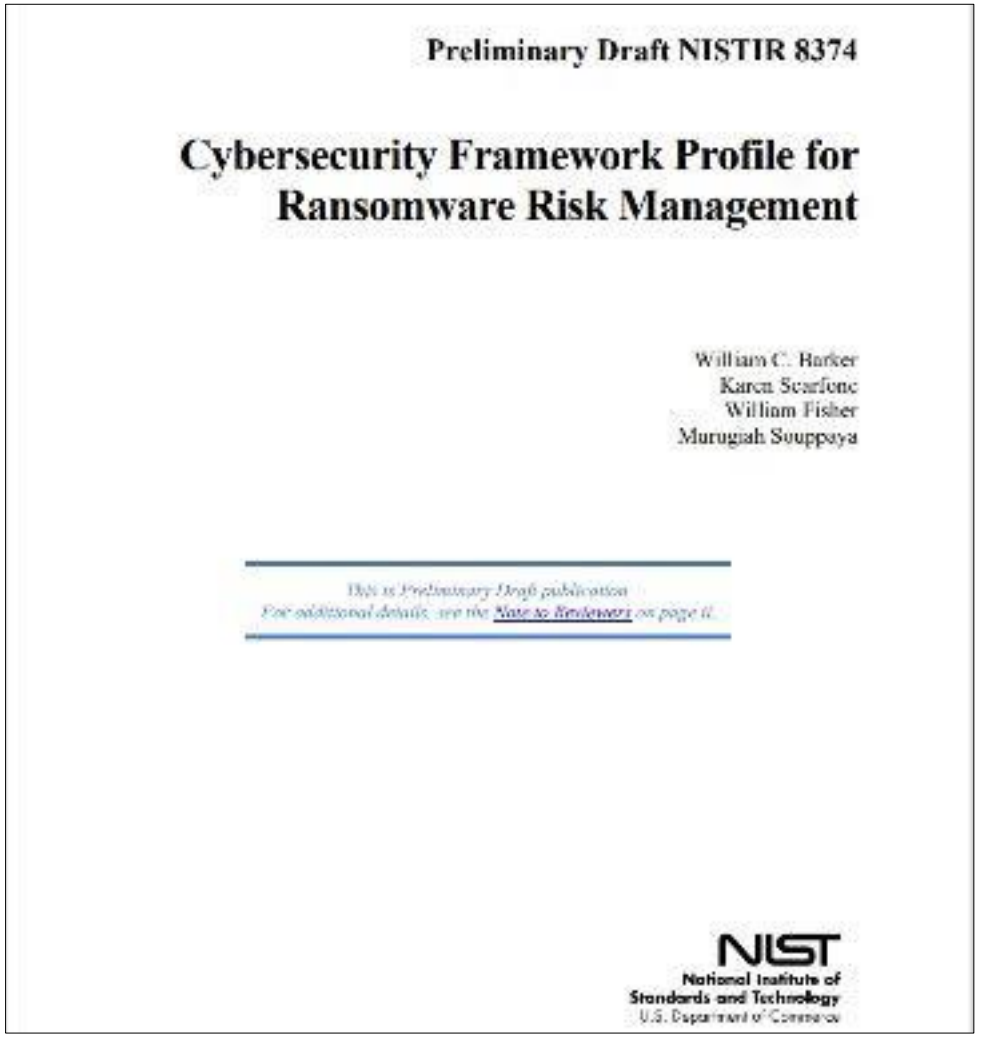
https://www.pymnts.com/news/security-and-risk/2021/white-house-ransomware-task-force-tries-to-stem-the-tide-of-attacks

Stop Ransomware Site



https://www.cisa.gov/stopransomware

NIST Guidance



The Ransomware Profile defined in this report **maps security objectives** from the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 [1] (also known as the Cybersecurity Framework) to security capabilities and measures that support preventing, responding to, and recovering from ransomware events. The profile can be used as **a guide to managing the risk of ransomware events**. That includes helping to gauge an organization's level of readiness to **mitigate ransomware threats** and to react to the potential impact of events. The profile can also be used to identify opportunities for improving cybersecurity to help thwart ransomware.

Reviews actions agencies can take each of the five Cybersecurity Framework Functions:

- Identify
- Protect
- Detect
- Respond
- Recover

https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf

Defensive Best Practices

- Employ **MFA** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- Apply the principle of **least privilege** to all systems and services so that users only have the access they need to perform their jobs
- Leverage best practices and enable security settings in association with cloud environments
- Employ logical or physical means of **network segmentation** to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology.
- Ensure your organization has a comprehensive **asset management** approach.
- **Restrict usage of PowerShell**, using Group Policy, to specific users on a case-by-case basis
- **Secure domain controllers (DCs).** Threat actors often target and use DCs as a staging point to spread ransomware network-wide.
- Retain and adequately **secure logs** from both network devices and local hosts.
- **Baseline and analyze network activity** over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal vs anomalous account activity).

Multi-State Information Sharing and Analysis Center (MS-ISAC) Ransomware guide: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

Role of AI/ML in Cybersecurity

How AI and ML Affect CyberSecurity?

- With the advancement in the field of AI and ML, new methodologies are being introduced to make the cybersecurity domain automated and risk-free.

  - **Anomaly Detection**
  - **Detects Malicious Attacks**
  - **Email Monitoring**

https://www.globaltechcouncil.org/artificial-intelligence/a-quick-guide-the-role-of-ai-and-ml-in-cybersecurity/

Collaboration

- Cybercrime is a global issue requiring a global response. Diplomacy and legal frameworks must be worked out and soon.
  - US President has issued a warning to Russia on critical infrastructure
  - Key cyber positions filled at WH, DHS, and DoS
  - Criminals are being identified, sanctioned and in some cases prosecuted
  - Awesome work by FBI, CISA, NSA, FINCEN, and others
- The private sector must work with Government before and earlier during attacks, share information, and work together to recover from the event
- The "*community of nations*" must decide what threshold must be crossed before we respond (cyber or otherwise) against either the criminals, or nation states who harbor or employ them.

FBI Claws Back Millions of DarkSide's Ransom Profits


NSA, CISA and FBI Issue Cybersecurity Advisory in Response to the People's Republic of China's Deployment of State-sponsored Malicious Cyber Activity

Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe

Questions

Dr. William Butler

Department Chair

Cyber and Information Security Programs

Email: whbutler@captechu.edu

Phone: 240-965-2458

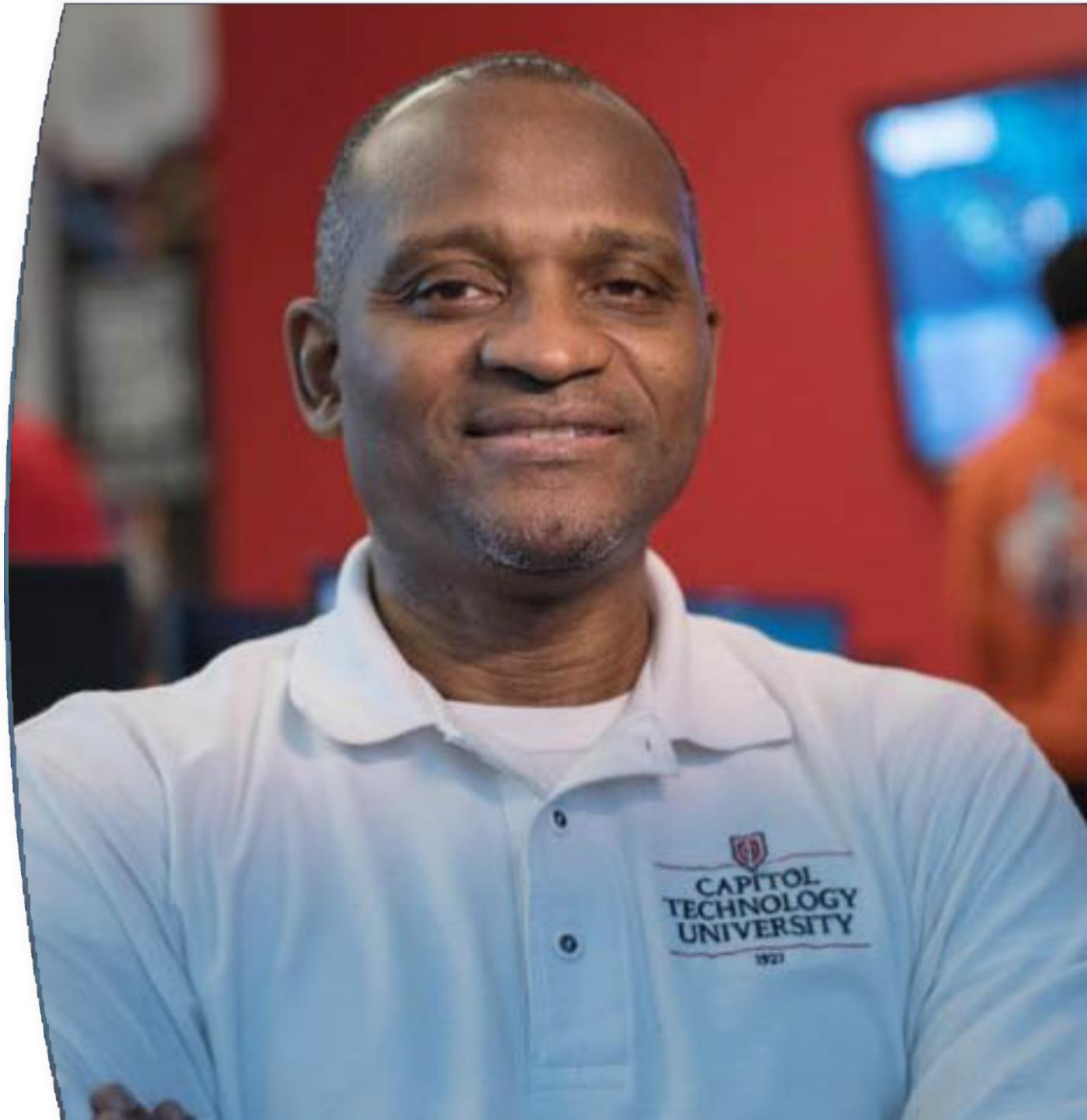
Thank You

“The Ransomware Threat”

Dr. William Butler

Chair, Cyber and Information Security,
Director, Center for Cybersecurity
Research and Analysis (CCRA)

Capitol Technology University

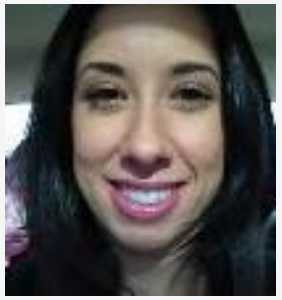


Panel
Malware & Ransomware –Why do they matter?

Panelists

Steven Hernandez
CISO - Director
Information Assurance Division - Department of Education

Mychael Brown
Senior SOC Engineer
Electrosoft Services, Inc.



Yvonne D Rivera
Co-Founder, CEO
CyberMyte, LLC

Togai Andrews
CISO
Bureau of Engraving and Printing – Department of The Treasury

Inno Eroraha
Founder & Chief Architect
NetSecurity Corporation

Moderator

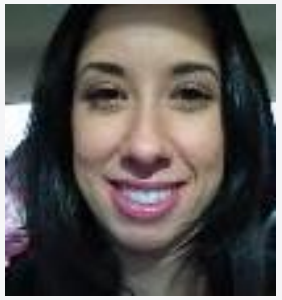
Pete Tseronis
Founder & CEO - Dots and Bridges LLC

Thank You!

Panelists

Steven Hernandez
CISO - Director
Information Assurance Division - Department of Education

Mychael Brown
Senior SOC Engineer
Electrosoft Services, Inc.



Yvonne D Rivera
Co-Founder, CEO
CyberMyte, LLC

Togai Andrews
CISO
Bureau of Engraving and Printing – Department of The Treasury

Inno Eroraha
Founder & Chief Architect
NetSecurity Corporation

Moderator

Pete Tseronis
Founder & CEO - Dots and Bridges LLC

Conference Remarks

- Brief Survey
- Recording available “on demand”
- Thank you!

Malware/Ransomware Cybersecurity Insights

Dr. Sarbari Gupta

CEO

Electrosoft Services, Inc.

Electrosoft

Dr. Bradford L. Sims

PRESIDENT
Capitol Technology University

CAPITOL
Technology University

Thanks to the Event Sponsor

Developer of **ThreatResponder**, an endpoint threat protection platform.

Electrosoft

CAPITOL Technology University

Thank You!

Electrosoft and CAPITOL Technology University