Week of October 21, 2024

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources

The Pennsylvania State University Agrees to Pay $1.25M to Resolve False Claims Act Allegations Relating to Non-Compliance with Contractual Cybersecurity Requirements

www.justice.gov

The Pennsylvania State University (Penn State), located in University Park, Pennsylvania, has agreed to pay $1,250,000 to resolve allegations that it violated the False Claims Act by failing to comply with cybersecurity requirements in fifteen contra...

Engaging with Security Researchers: Embracing a “See Something, Say Something” Culture

www.cisa.gov

n an age where digital systems have an electronic tendril in nearly every aspect of our lives, the role of cybersecurity researchers is more important than ever. These individuals and groups proactively identify weaknesses in software, networks, and hardware, often before malicious actors get a chance to exploit them...

Cybersecurity Awareness Month

www.nist.gov

NIST Cybersecurity Program
Cybersecurity Awareness Month — celebrated every October — was created in 2004 as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online.

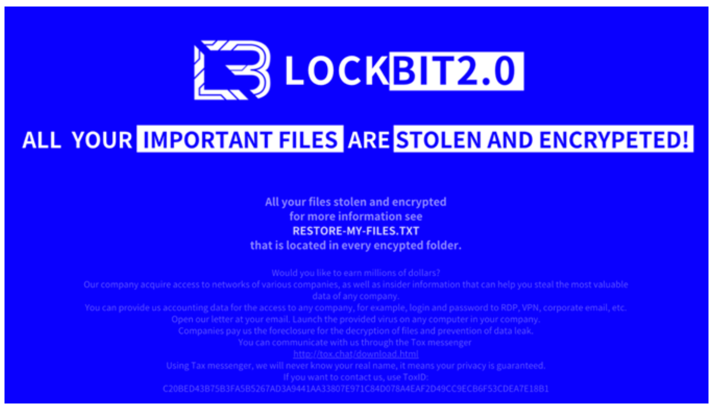
NASPO and NASCIO Release Joint Report on AI in Public Procurement - NASCIO

www.nascio.org

Lexington, KY, Tuesday, October 15, 2024 – The National Association of State Procurement Officials (NASPO) and the National Association of State Chief Information Officers (NASCIO) are pleased to announce the release of their joint publication, AI-Po...

Cybercrimes, Scams & Incidents

Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks



LOCKBIT2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPETED!

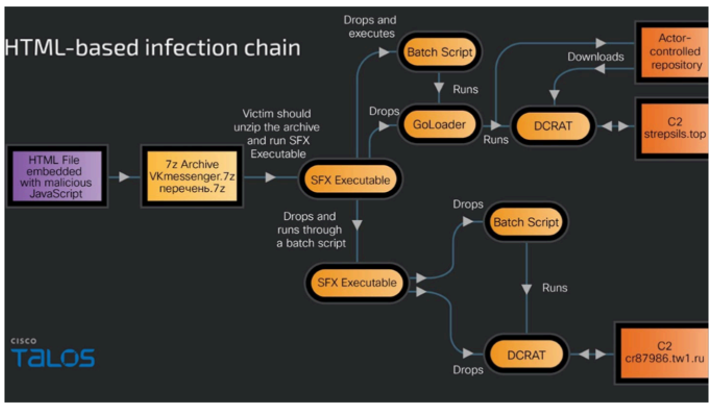
All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
http://tox.chat/download.html
Using Tax messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
C20BED43B75B3FA5B5267AD3A9441AA33807E971C84D078A4EAF2D49CC9ECB6F53CDEA7E18B1

Ransomware Gangs Use LockBit's Fame to Intimidate Victims in Latest Attacks

thehackernews.com

Threat actors exploit Amazon S3 in ransomware attacks, using AWS credentials for data theft.


HTML-based infection chain
HTML File embedded with malicious JavaScript
7z Archive VKmessenger.7z перечень.7z
Victim should unzip the archive and run SFX Executable
SFX Executable
Drops and executes
Batch Script
Runs
Drops
GoLoader
Runs
DCRAT
Downloads
Actor-controlled repository
C2 strepsils.top
Drops and runs through a batch script
SFX Executable
Drops
Batch Script
Runs
Drops
DCRAT
C2 cr87986.tw1.ru
CISCO TALOS

Gophish Framework Used in Phishing Campaigns to Deploy Remote Access Trojans

Industry News

Headlines collected from across the cybersecurity industry related to legislation, business, and big tech

Columbus, Ohio's messy ransomware saga underscores legal gray areas | StateScoop

statescoop.com

Countless ransomware attacks against government agencies have followed a familiar pattern, but Columbus, Ohio's has been messier.

SEC Charges Four Companies Over Misleading Disclosures on SolarWinds Hack

www.securityweek.com

The SEC announces penalties against Unisys, Avaya, Check Point and Mimecast for downplaying the impact of the SolarWinds Orion hack.

thehackernews.com

A new phishing campaign targets Russian-speaking users, spreading DCRat and PowerRAT via Gophish toolkit.

Internet Archive breached again through stolen access tokens

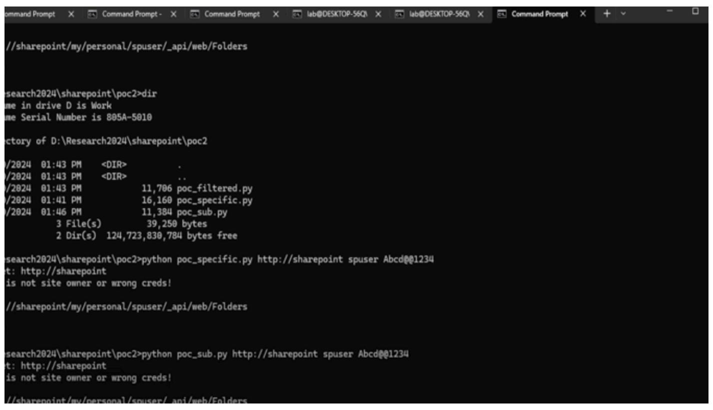
www.bleepingcomputer.com

The Internet Archive was breached again, this time on their Zendesk email support platform after repeated warnings that threat actors stole exposed GitLab authentication tokens.

Change Healthcare data breach officially affects 100M people

www.cybersecuritydive.com

The breach is the largest ever reported to a portal managed by federal regulators.



```
//sharepoint/my/personal/spuser/_api/web/Folders



search2024\sharepoint\poc2>dir
me in drive D is Work
me Serial Number is 805A-5010

ctory of D:\Research2024\sharepoint\poc2

/2024  01:43 PM    <DIR>          .
/2024  01:43 PM    <DIR>          ..
/2024  01:43 PM            11,706 poc_filtered.py
/2024  01:41 PM            16,160 poc_specific.py
/2024  01:46 PM            11,384 poc_sub.py
          3 File(s)         39,250 bytes
          2 Dir(s)  124,723,830,784 bytes free

search2024\sharepoint\poc2>python poc_specific.py http://sharepoint spuser Abcd@@1234
t: http://sharepoint
is not site owner or wrong creds!

//sharepoint/my/personal/spuser/_api/web/Folders



search2024\sharepoint\poc2>python poc_sub.py http://sharepoint spuser Abcd@@1234
t: http://sharepoint
is not site owner or wrong creds!

//sharepoint/my/personal/spuser/_api/web/Folders
```

CISA Warns of Active Exploitation of Microsoft SharePoint Vulnerability (CVE-2024-38094)

thehackernews.com

CISA alerts on active exploitation of a SharePoint flaw, urging federal agencies to apply patches quickly.

CISA proposes new security requirements to protect govt, personal data

www.bleepingcomputer.com

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) is proposing security requirements to prevent adversary states from accessing American's personal data as well as government-related information.

The Global Surveillance Free-for-All in Mobile Ad Data

krebsonsecurity.com

Not long ago, the ability to digitally track someone's daily movements just by knowing their home address, employer, or place of worship was considered a dangerous power that should remain only within the purview of nation states. But a new lawsuit in a likely constitutional battle over a New Jersey privacy law shows that anyone can now access this capability, thanks to a proliferation of...

***Please be advised that** the following resources and materials are for informational purposes only. **The opinions and views expressed in these materials** are the opinions of the designated authors and do not reflect the opinions or views of **the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth).** The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.*

Official Quick Links

- CISA
- CIS/MS-ISAC
- CyberCom
- DHS
- DOJ
- FBI
- NIST
- NSA
- White house | ONCD

External Quick links

- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record