NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | January 7, 2016

Threat Analysis - January 7
Cyber Attack Implicated in Ukraine Power Outage

TLP **WHITE** | ***Intelligence agencies and cybersecurity researchers are investigating a power outage that occurred in Western Ukraine on December 23, specifically whether or not malware discovered on the targeted utility's network played a direct role in impacting the electric grid.*** If malware is confirmed to have caused the outage, opposed to human error or equipment failure, this would mark the first documented power disruption resulting from a cyber attack. Though this incident was likely targeted, posing no direct threat to US infrastructure, it underscores the susceptibility of industrial systems that distribute critical resources. Moreover, it demonstrates the willingness of sophisticated actors, whether state-sponsored or inspired, to conduct attacks which impose significant consequences on civilian populations, as well as governments.

Read the full threat analysis

NJCCIC Blog: Don't Get Harpooned by a Whaling Attack

Unlike phishing attacks which cast a wide net in the hopes of catching as many victims as possible, whaling is a term used to describe carefully crafted emails designed to target or spoof specific people within an organization – usually top level executives, upper management, and other corporate decision-makers. Read this week's Cyber Blog to learn how to protect yourself and your organization

Latest Cyber Alerts

Multiple Vulnerabilities in Google Android

Cyber News

Comcast's Xfinity Home Security vulnerable
via CSO Online

Well-informed tech support scammers target Dell users
via NetSecurity

The Father of Online Anonymity Has a Plan

from whaling attacks.

Read full blog post here

Breach Notification

Time Warner Cable

On Wednesday, Time Warner Cable Inc. announced that up to 320,000 customers' email addresses and passwords may have been compromised in the breach of third-party organization. Time Warner customers are urged to change their passwords as a precaution.

NJCCIC Cyber Alert

End of Life (EOL) notices are provided when companies announce that they will no longer provide security updates, hot fixes, or technical support for select software or software versions. This information is provided here, as the failure to properly upgrade EOL software in a timely manner may potentially subject the organization to a higher level of risk, thus increasing the potential for compromise. MS-ISAC recommends organizations inventory their systems to determine if this software is still in use, and if so, if it is connected to the Internet. A proper migration plan should be developed to ensure the software is upgraded to a supported product.

- Microsoft will discontinue support on January 12, 2016, for versions of Internet Explorer prior to version 11 and for

to End the Crypto War
via Wired

Researchers Out Default Passwords Packaged With ICS/SCADA Wares
via Dark Reading

Meet Ransom32: The first JavaScript ransomware
via Emsisoft

Tip of the Week

"Securing Your Home Network"

Home routers have become an integral part of our global communications footprint as use of the Internet has grown to include home-based businesses, telework, schoolwork, social networking, entertainment, and personal financial management. Routers facilitate this broadened connectivity. Most of these devices are preconfigured at the factory and are Internet-ready for immediate use.

Read more about this cyber tip and others from US-CERT

Questions?

Email a Cyber Liaison Officer at njccic@cyber.nj.gov.

Connect with us!

versions 4, 4.5, and 4.5.1 of the .NET Framework.
- Microsoft will discontinue extended support for SQL Server 2005 on April 12, 2016. (Of note, multiple versions of .NET can be installed on a single machine.

---

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell

DISCLAIMER: This bulletin is provided as is for informational purposes only. The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) and the Regional Operations Intelligence Center (ROIC) do not provide any warranties of any kind regarding any information contained within. The NJCCIC and ROIC do not endorse any commercial product or service, referenced in this bulletin or otherwise. Further dissemination of this bulletin is governed by the Traffic Light Protocol (TLP). For more information about TLP, see https://www.us-cert.gov/tlp/.