NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | October 28, 2015

New Jersey Cyber Incident:

NJ Business Infected with Point-of-Sale Malware

TLP: **WHITE** | ***On October 13, 2015 a New Jersey business discovered an infection of a point-of-sale (PoS) malware variant, detected by antivirus software as lanst.exe, one of many variants commonly known as Dexter.*** It remains definitively unclear how an employee's laptop was initially exposed to the malware, though the NJCCIC assesses it was likely via a spear-phishing or drive-by download tactic. In this instance, the malware exploited the business' lack of two-factor authentication and 'flat' network—meaning there was no segregation between various components—as well as outdated computer systems and weak security policies. There is currently no evidence that any business or customer data was exfiltrated from the network.

Threat Analysis

October 28, 2015

SQL Injection: A Common, Yet Avoidable, Attack Vector

The NJCCIC assesses that organizations using Structured Query Language (SQL) for database management systems are at a high risk for SQL injection (SQLi) attacks unless the appropriate mitigation strategies are applied. SQL is the standard computer language used to conduct various functions such as querying and modifying data in relational database management systems. SQLi is a cyber tactic that exploits a vulnerability in a database application that

Latest Cyber Alerts

Vulnerability in Adobe Shockwave Player Could Allow for Arbitrary Code Execution

Multiple Vulnerabilities in Apple Products Could Allow Remote Code Execution

NJ Cyberlog

Keeping Your Children Safe Online

The Internet is certainly an invaluable tool, but with its many advantages come very real threats and potentially severe consequences. The Internet can be a very hazardous place for children who are naturally trusting of

does not properly validate or encode user input.

Tip of the Week

"Malware Wears Costumes, Too"

Much like trick'r'treaters and other Halloween mischief makers, malware can use "costumes" to disguise what it is and to trick you into installing it. These 'costumes' come in many forms but if you know what to look for, you can avoid the tricks.

- Only open an email attachment or click on a link if you're expecting it and know what it contains.
- If something looks suspicious in an email from a trusted source, call and verify the email is legitimate.
- Use up-to-date anti-virus protection and apply recommended patches/updates to your device.
- Use discretion when posting personal information on social media. This information is a treasure-trove to scammers who will use it to feign trustworthiness.

others and who can't predict or even comprehend the potential long-term ramifications of their online actions. With all the devices that can give your children unfettered access to the Internet, now is the time to sit down with them and have a serious conversation about Internet safety. We at the NJCCIC understand that it might be difficult to start the conversation and to figure out what to say and do.

In Case You Missed It

Webinar - Your Evolving Digital Life

Cyber Threat Intelligence Analysts from the NJCCIC discussed the best practices and resources that everyone can take advantage of to avoid the most common threats facing Internet users, such as malware infections and account compromises, in the last NJCCIC webinar during National Cyber Security Awareness Month.

You can find all #NJCyber Webinars from October and more at cyber.nj.gov/webinars.

Follow @NJCybersecurity on Twitter to get daily tips, resources and analysis throughout October as part of National Cyber Security Awareness Month.

Connect with us!

---

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/.

View this email **online**.

communications@njohsp.gov
Trenton, NJ | 08625 US