NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | December 2, 2015

Alert: Angler Exploit Kit Leading to Various Payload Downloads

Over the last 24 hours, the NJCCIC has detected a series of successful Angler exploit kit infections which have resulted in the download of various malware payloads and backdoor connections. We have not yet determined the initial vector for the Angler connections, however, we assess it is likely spear-phishing and/or drive-by downloads. For a list of the malicious IP addresses and URLs associated with this Angler exploit kit traffic:

Read More Here

Preventative Measures: The NJCCIC recommends organizations implement awareness training for all employees so users at every level can identify malicious phishing emails and practice safe-browsing techniques to avoid malicious websites and malvertising. Users should be trained to never click on links or download attachments in unsolicited emails. Spear-phishing tactics are continuously evolving and becoming more sophisticated and effective, therefore, regular training is required to ensure users are aware of the most current threats. Additionally, all endpoints must be kept up-to-date with the latest security patches for all operating systems, software applications, web browsers, and plugins. Any non-essential applications or plugins should be disabled or uninstalled.

NJCCIC Announcements

Two Governor Christie Administration officials visited with 200 senior citizens to raise awareness of cybersecurity threats and educate them about ways to protect themselves against attacks and scams,

Latest Cyber Alerts

[Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution]

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the especially during the holiday shopping season.

Read More Here

browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

Breach Notification

Children's Toymaker VTech Announces Large-Scale Breach

The Hong Kong-based maker of digital children's toys, VTech, has acknowledged a breach involving personal information of 4.8 million parents and 6.3 million children, of which the vast majority were US-based customers. The hacked data includes names, email addresses, passwords, and home addresses of the parents, and first names, genders and birthdays of their children users. The hacker was also able to obtain thousands of pictures of parents and kids, as well as a year's worth of chat logs. Media reporting indicates the hacker exploited a SQL injection (SQLi) vulnerability in the company's databases to access and exfiltrate the data. For more information on SQLi, please read our threat analysis product on this common, yet avoidable, exploit tactic.

NJCCIC Comment: The alleged hacker has expressed no interest in releasing or selling the stolen data, and there were no Social Security numbers or financial information stolen, therefore victims are not at risk for identity theft or fraud. However, malicious actors are likely to capitalize on the breach by targeting victims with spear-phishing emails crafted to appear as if they come from VTech or in some way related to the breach. These phishing attempts are likely to ask users to click a link in order to change their passwords, update their profiles, or sign up for complimentary credit-monitoring. The NJCCIC recommends users never click on links or attachments in unsolicited emails, and instead visit the official page of the targeted organization for up-to-date information.

This incident underscores the lack of data-level protections among companies that collect and store large amounts of personal information on their customers. The NJCCIC highly recommends that any organization which collects and stores customer's personal or financial data implement encryption of data at rest and in transit. For organizations with limited resources, or the need to secure various legacy systems, an alternative to complex encryption implementations is tokenization. For some organizations, a combination of tokenization and encryption may be the most practical solution to minimize risk.

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/.