**TLP: WHITE**

**MS-ISAC CYBER ALERT**

**TO: All MS-ISAC and IIC Members**

**DATE ISSUED:**10/10/2013

**SUBJECT:** Spear Phishing Emails Targeting State Executives

The MS-ISAC SOC was notified by a trusted third party about spear phishing emails targeting State Executives, including Fusion Center Directors. These emails contain a virus as an attachment and a spoofed sender address.

**Sample Email Indicators:**

Subject:            “Annual Form - Authorization to Use Privately Owned Vehicle on State Business”

Attachment:      Attachments follow the naming convention of “Form\_[Varying Digits and Numbers].zip. For example: Form\_nfcausa.org.zip, Form\_20130810.exe, Form\_f4f43454.com.zip.

Spoofed Sender: “[fraud@aexp.com](mailto:fraud@aexp.com)” “[Dewayne@nfcausa.org](mailto:Dewayne@nfcausa.org)”

Sender IP:         209.143.144.3

Sender Host:     mail.netsential.com

The attachment is currently being detected by all of the major AV products with various names including ZBot, Cutwail and Kazy. If the malware is installed, it will attempt to connect to warehousesale[dot]com[dot]my on port 443/TCP.

**Recommendations:**

We recommend the following actions be taken:

·         If traffic is identified, notify MS-ISAC immediately for further assistance

·         Since these emails are originating from spoofed email accounts, educate your users on checking the senders of the e-mails and verify the legitimacy of the sender

·         Block traffic to the above domain at your network perimeter devices

·         Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources

·         Remind users to be cautious when clicking on links in emails coming from trusted sources

·         Ensure anti-virus is installed and definitions are up to date

**References:**

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31177>

<http://blog.mxlab.eu/2013/10/08/email-annual-form-authorization-to-use-privately-owned-vehicle-on-state-business-contains-new-trojan-variant/>

The Center for Internet Security

31 Tech Valley Drive

East Greenbush, NY 12061

518-266-3488

7x24 SOC 1-866-787-4722

**TLP:WHITE**

**TLP: WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp>

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.   
. . .