NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Advisory

"Night Dragon"

Initial Distribution: February 18, 2011

Publicized increase in coordinated covert cyber exfiltrations targeting global oil, energy, and petrochemical companies, dubbed "Night Dragon."

Why am I receiving this? >>
About NERC Alerts >>

Status:	**No Reporting is Required – For Information Only**
	**PUBLIC:** No Restrictions **More on handling >>**
Instructions:	NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure, for such use as your organization deems appropriate. **No particular response is necessary.** This NERC Advisory is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Advisory. Additionally, issuance of this Advisory does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the Advisory if such failure constitutes a violation of a Reliability Standard.
Distribution:	**Primary Distribution: Primary Compliance Contacts** Reliability Coordinator, Balancing Authority, Transmission Operator, Generation Operator, Generation Owner, Transmission Owner, Planning Authority (Coordinator), Load-Serving Entity, Distribution Provider, Purchasing-Selling Entity, Interchange Authority, Reserve Sharing Group, Transmission Planner, Transmission Service Provider, Resource Planner **Who else will get this alert? >>** **What are my responsibilities? >>**
Primary Interest Groups:	Chief Security Officer, Information Security Officer, Industrial Control System Engineers
Advisory:	NERC is issuing an Advisory to industry on the publicized increase in coordinated covert cyber attacks targeting global oil, energy, and petrochemical companies, dubbed "Night Dragon." Research has indicated that these attacks started in November 2009 and that five, possibly as many as twelve, oil and gas companies were compromised. The exploits and methods contained in Night Dragon's attack set are not new or unique to our industry, nor are the approaches or methods

to combat it. However, it is a reminder of the importance of implementing cyber security best practices to protect against such attacks. NERC is releasing this Advisory in response to an identified pattern of activity that has been directed against the energy sector. The Advisory contains specific information and suggested actions for Night Dragon in accordance with standard detection, prevention, and recovery phases of a strong incident response program.

The ES-ISAC estimates that the risk to bulk power system reliability from this vulnerability is MEDIUM, due to the fact that exploit code is available, complexity is low, and evidence shows attacks are targeted. Although financial data appear to be the primary target, successful exploits may include Industrial Control and SCADA systems. The goal of the attacks is data theft, which bears a lower reliability risk than a denial of service attack on the systems that control and operate the bulk power system.

Background:

Evidence shows that Night Dragon may have originated in the Shandong Province of China.

These attacks appear to have had some success in evading detection by standard security software and network policies due to the fact that tools used to launch the attacks utilize a number of exploit techniques and ultimately employ administrative credentials.

Six specific attack vectors have been identified below, each with a definition and general protection information. NERC also provides specific suggested actions in the attached document for those who may wish to pursue them.

1. Social engineering – Similar to old “con man” strategies, social engineering attacks trick users into performing an act that provides the attacker with confidential information or unauthorized access to the user’s network. Attackers often speak with disarming authority and appear legitimate to unsuspecting users who are then lured into divulging sensitive information or browsing to a certain web page for further instructions. Although decades old, social engineering attacks are still effective attack tools and end user training is critical to remind them to be wary of such attacks and report suspicious calls. Other controls may include authentication and dial-back technologies.

2. Spearphishing – is a more directed and customized form of old phishing scams. Spearphishing targets specific recipients or groups with personalized messages that appear legitimate and that seem to originate from a trusted source via the use of special masquerading software in combination with information obtained

through social engineering or other reconnaissance. Similar to social engineering attacks, the goal of spearphishing is to obtain confidential information or unauthorized access to the user's network by tricking unwitting users into performing an act, such as clicking on an attachment containing the malicious code or browsing to a malicious website. End user training is a primary control to protect against spearphishing. Sanctioned penetration testing that utilizes social engineering and spearphishing attacks are excellent tools to validate and reinforce user training and effectiveness. Strong email and content filters are also useful controls to defeat spearphishing attacks.

3. Host O/S exploits – Security vulnerabilities inherent in the endpoint operating systems exist, such as un-patched applications with buffer overflows, SQL injection vulnerabilities and weak authentication. Use of end-of-life, unsupported operating systems and applications provide additional attack vectors because security patches are no longer available.

4. Endpoint Protections – No security posture can be considered robust or sufficient without particular attention to endpoint protection. System images must be minimized and hardened; endpoint security controls must be utilized; security patches must be kept up to date; vulnerability and penetration testing must be employed; and end users must be sufficiently vetted and trained to avoid circumventing endpoint protections.

5. Active Directory (AD) compromises – Directory services such as AD and LDAP are very powerful system management tools. However, their compromise would also provide a powerful tool to a potential attacker. AD vulnerabilities are well known (see MS-ISAC advisory 2009-034 for example) and exploit code is readily available. AD must be securely configured, patched, and regularly monitored for potential security issues.

6. Remote administration tools (RATs) – RATs are commonly used system administrative tools that allow administrators to manage remote computers. One such tool, popular among attackers, is zwShell. Hackers routinely use RATs to manage victims' computers and completely control their use and function. Features of RATs commonly include screen and webcam spying, keystroke logging, mouse control, file/registry manipulation, process management, and remote command shell capability. Industry best practices for network and host security mechanisms offer the best protection against RAT exploitation. Strong authentication must be enabled on border devices, internal network appliances and endpoints; robust access control methods must be implemented, including blacklisting known IP addresses

of origination and destination; intrusion detection systems and other behavioral awareness tools such as event correlation engines must be employed; and security controls must be validated through routine maintenance, testing and exercises.

NERC and its federal partners jointly developed the attached document that provides specific protection steps for those who may wish to assess or reduce their exposure to this threat.

Contact:

Tim Roxey
Director of Critical Infrastructure Risk Management and Technology Division
North American Electric Reliability Corporation (NERC)
1120 G Street NW, Suite 990
Washington, DC 20005
Telephone: (410) 586-0026
Fax: (202) 393-3955
Tim.Roxey@nerc.net

To report any incidents related to this alert, contact:
ES-ISAC 24-hour hotline
609.452.1422
esisac@nerc.com