Attachment 1 - Night Dragon Specific Protection Measures for Consideration

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 NERC issues this Advisory in response to an identified pattern of activity that has been directed against the energy sector. This Advisory communicates specific information and suggested actions for Night Dragon in accordance with standard detection, prevention, and recovery phases of a strong incident response program.

The following framework provides two sets of prioritized measures and countermeasures that may be useful to prevent traffic to and from known "command and control" (C&C) servers and domains, and identify the presence of Night Dragon activity on specific systems. They begin with simple low-cost, low-impact, high-value prevention and detection suggestions, and escalate to more invasive actions should evidence of Night Dragon activity or compromise be found.

These actions are based on information available as of February 18, 2011, and while they offer good suggestions to detect and combat Night Dragon, they provide no guarantee that a targeted attack against your systems would be unsuccessful. If you have not already done so, take this opportunity to establish a reporting relationship with ICS CERT and NERC's ES-ISAC for real-time sharing of any new information on this attack set such as additional C&C servers, updated search strings, new variants, etc.

Entities should also closely monitor their relevant security vendors for signature updates and detection and removal tools. Some of these measures are invasive and could create problems with operational systems. It is important to understand your technology environment and the impact these tools could have on operational systems prior to any deployment.

Primary Protection and Discovery Measures

The following three actions are important first steps in detecting and preventing known Night Dragon activity.

1. Apply access control restrictions on all perimeter devices.
    a. Modify email blacklists and firewall Access Control Lists ACLs to deny, log and alert on traffic to/from the following primary domains used by the known C&C servers. And, according to McAfee[1] all four domains have been used frequently by other Malware so blocking them may be warranted regardless.
        i. is-a-chef.com
        ii. thruhere.net
        iii. office-on-the.net

[1] http://www.mcafee.com/us/about/night-dragon.aspx?cid=WBB009

iv. selfip.com.

b. Modify Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and other deep-packet inspection tools to detect and alert on network traffic associated with Night Dragon activity. If detected, validate as malicious and consider blocking the traffic in addition to triggering an alert:

   i. Each communication packet between compromised hosts and the C&C servers are signed with a plain text signature of "hW$." (Or "\x68\x57\x24\x13") at the byte offset 0x0C within the TCP packet.

   ii. Backdoor beacon, identified by a 5-second interval with an initial packet with the pattern: "\x01\x50[\x00-\xff]+\x68\x57\x24\x13."

   iii. Beacon acknowledgement with the pattern: "\x02\x60[\x00-\xff]+\x68\x57\x24\x13."

   iv. Periodic heartbeat or keep-alive signal with the pattern: "\x03\x50[\x00-\xff]+\x68\x57\x24\x13."

   v. Plaintext password exchange with the pattern: "\x03\x50[\x00-\xff]+\x68\x57\x24\x13."

c. Open source IDS signatures have been made available on a number of open source websites and added to open source rule sets. Some commercially available IDS / IPS signatures have also been updated to include Night Dragon detection.

   i. CISCO specific information can be found here: *http://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=33819&signatureSubId=0*

   ii. SNORT specific information can be found here:

   http://www.snort.org/vrt/docs/ruleset_changelogs/2_9_0_4/changes-2011-02-10.html

d. Identify and examine any hosts generating suspected Night Dragon traffic and take necessary action to respond and recover.

e. Maintain vigil for additions to Night Dragon's C&C server and signature lists and quickly update your defenses accordingly.

2. While there is no "patch" for Night Dragon, as a preventative measure ensure that security patches on all servers are up to date, especially for external-facing web servers as they are primary attack vectors.

3. Conduct keyword searches or "greps" of current and archived perimeter logs looking for signs of traffic to/from the known C&C servers (e.g. "find 'is-a-chef.com'" or "grep 'is-a-chef.com' /logfilename"). Examine both ICS and corporate network perimeter logs and as far back as possible to the dates recommended by the MacAfee whitepaper.

Secondary Protection Measures

For entities wishing to pursue a more vigorous course of action or if entities discover evidence of Night Dragon activity or compromises using the previous steps, the following actions may be useful in helping to determine compromises at the host level.

1. Review any systems/networks with trust relationships and analyze the active communications paths from those assets.
2. Run host-based automatic detection tools capable of discovering related Malware on all hosts. Examples of free tools include *Stinger* and the *Night Dragon Vulnerability Scanner*, available at http://www.mcafee.com/us/downloads/free-tools/index.aspx
3. Search systems for the following command and control programs and eliminate as applicable:

Filename	MD5 Checksum
Shell.exe	093640a69c8eafbc60343bf9cd1d3ad3
zwShell.exe	18801e3e7083bc2928a275e212a5590e
zwShell.exe	85df6b3e2c1a4c6ce20fc8080e0b53e9

4. A Trojan dropper, which is a delivery mechanism for malware, is commonly used in Night Dragon attacks. It is usually executed through a PSEXEC or an RDP session and may leave valuable forensic information in system event logs. When executed, the dropper creates a temporary file that is reflected in Windows update logs ("KB*.log" files in "C:\Windows"). This temporary file may have limited usefulness, as it may disappear if a backdoor is successfully opened. Its lack of existence doesn't guarantee a system is free of infection.
5. A Trojan backdoor may exist as a DLL usually located in the %System%\System32 or %System%\SysWow64 directory. This DLL is a system or hidden file, 19 KB to 23 KB in size, and includes an XOR-encoded data section that is defined by the C&C application when the dropper is created. It includes the network service identifier, registry service key, service description, mutex name, C&C server address, port, and dropper temporary file name. The backdoor may operate from any configured TCP port.
6. Two potential Trojan backdoors:

Filename	MD5 Checksum
startup.dll	A6CBA73405C77FEDEAF4722AD7D35D60
connect.dll	6E31CCA77255F9CDE228A2DB9E2A3855

7. And finally, if compromises are suspected or discovered, work closely with your operating system and application vendors to ensure safe and complete eradication.