ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-041-01A —MCAFEE NIGHT DRAGON REPORT

UPDATE A

February 11, 2011

OVERVIEW

McAfee has published a white paper titled "Global Energy Cyberattacks: Night Dragon,"[a] which describes advanced persistent threat activity designed to obtain sensitive data from targeted organizations in the global oil, energy, and petrochemical industries. According to the report, this activity began in 2009 or potentially as early as 2007.

IMPACT

The threat McAfee identifies as Night Dragon focused specifically on the energy sector; however, the tools and techniques used by Night Dragon can be highly successful when targeting any industry. Other sectors may also be vulnerable and under similar persistent cyber espionage attacks.

BACKGROUND

According to the report, the attacks have been ongoing since November 2009 and involve social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of remote administration tools (RATs) in targeting and harvesting sensitive competitive proprietary operations, and project-financing information with regard to oil and gas field bids and operations.

McAfee reports that once the attackers have complete control of the targeted internal system, they dump account hashes with gsecdump and use the Cain & Abel tool to crack the hashes to leverage them in targeting other more sensitive information.

Exfiltrated files of interest focused on operational oil and gas field production systems and financial documents related to field exploration and bidding. In some cases, the files were copied to and downloaded from company web servers by the attackers. In certain cases, the attackers collected data from SCADA systems.

[a] McAfee, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf, accessed February 10, 2011.

MITIGATION

An outbreak or successful attack within your network can be detected through md5sum signatures and network packet signatures, which can be used within Intrusion Detection System (IDS) products from various commercial and open-source organizations.

COMMAND AND CONTROL APPLICATION

- Shell.exe 093640a69c8eafbc60343bf9cd1d3ad3
- zwShell.exe 18801e3e7083bc2928a275e212a5590e
- zwShell.exe 85df6b3e2c1a4c6ce20fc8080e0b53e9

TROJAN DROPPER

The Trojan dropper is a packaged executable customized to each victim that includes the dynamic link libraries (DLL) file and configuration settings for installing the backdoor on the remote system.

The dropper can be run from any directory and is usually executed with PSEXEC or an RDP session. Thus related Windows Security Event logs provide useful information concerning compromised Active Directory accounts. These logs can be reviewed with Windows Event Log Manager.

When executed, the dropper creates a temporary file that is reflected in Windows update logs (KB*.log files in c:\Windows folder).

The dropper is deleted when the backdoor is installed, and the temporary file is removed when the computer is restarted. If a backdoor has already been configured on the system, the dropper installation will fail.

TROJAN BACKDOOR

The Trojan backdoor consists of DLLs that appear under many other names.

These files have a correlated Windows Registry key that is determined by the dropper when the backdoor is installed. The dropper iterates through the Windows netsvcs registry keys and uses the first available key, indicating the path and filename of the backdoor in a ServiceDLL register. The backdoor operates as a service through a “svchost.exe netsvcs –k” registry setting. The service key can be found under:

HKLM\system\<controlset>\services\

The 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.

This DLL is specified in the ServiceDLL key in the related Windows netsvcs registry entry. The DLL is usually found in the %System%\System32 or %System%\SysWow64 directory.

TROJAN BACKDOOR 2

startup.dll A6CBA73405C77FEDEAF4722AD7D35D60

connect.dll 6E31CCA77255F9CDE228A2DB9E2A3855

Note: Connect.dll creates the temporary file "HostID.DAT," which is sent to the C&C server, then downloads and configures related DLLs including:

- PluginFile.dll
- PluginScreen.dll
- PluginCmd.dll
- PluginKeyboard.dll
- PluginProcess.dll
- PluginService.dll
- PluginRegedit.dll

Thereafter "Startup.dll" operates the service under a Windows Registry key. All communications seen so far with this version have been on Ports 25 and 80 over TCP but can operate on any determined port.

The service key is identified in the DLL (which does not include any encrypted data) as:

HKLM\Software\RAT

This DLL is usually found in the %System%\System32 directory; however, it has also been found in other locations. The path to the backdoor DLL is indicated in the Windows Registry ServiceDLL key.

NETWORK COMMUNICATIONS

--------- Begin Update A ----------

Network communications are relatively easy to detect because the malware uses a unique host beacon and server response protocol. Each communication packet between the compromised host and the C&C server is signed with a plain text signature of "hW$." (or "\x68\x57\x24\x13") at the byte offset 0x0C within the TCP packet.

---------- End Update A ----------

BACKDOOR BEACON

The backdoor begins its beacon at approximately 5-second intervals with an initial packet that may be detected with the pattern: "\x01\x50[\x00-\xff]+\x68\x57\x24\x13."

BEACON ACKNOWLEDGMENT

The server acknowledges the beacon with an initial response of "\x02\x60[\x00-\xff]+\x68\x57\x24\x13."

PASSWORD SENT BY BACKDOOR

The backdoor sends the password to the server in clear text after the server acknowledges the connection messages that can be detected with: "\x03\x50[\x00-\xff]+\x68\x57\x24\x13."

KEEP-ALIVE

While the backdoor and the server have an active connection, the backdoor will send "keep-alive" messages that can be detected with: "\x03\x50[\x00-\xff]+\x68\x57\x24\x13."

DOMAINS UTILIZE DYNAMIC DNS

The attackers use "dynamic DNS" Internet name services accounts to relay C&C communications or temporarily associate DNS addresses with remote servers. Primary domains that have been used for C&C traffic include (all of these have been used frequently by other malware):

- is-a-chef.com
- thruhere.net
- office-on-the.net
- selfip.com

ICS-CERT recommends organizations monitor and audit levels of access from extranets and DMZ servers to internal networks.

ADDITIONAL DETECTION TECHNIQUES

The backdoor beacons with its corresponding C&C server as long as the related address is active. If the address is abandoned or unreachable, the backdoor stops beaconing after some undetermined interval. When a compromised computer is restarted, however, the beaconing begins again because it is registered as a service in the Windows Registry. Antivirus may detect the Trojan unless it is beaconing or a full file system scan is performed.

SUMMARY

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[b]

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov

Toll Free: 1-877-776-7585

For Control System Security Program Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

[b] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html.