White Paper

Global Energy Cyberattacks: “Night Dragon”

By McAfee® Foundstone® Professional Services and McAfee Labs™

February 10, 2011

Table of Contents

Executive Summary

In 2010, we entered a new decade in the world of cybersecurity. The prior decade was stained with immaturity, reactive technical solutions, and a lack of security sophistication that promoted critical outbreaks, such as Code Red, Nimda, Blaster, Sasser, SQL Slammer, Conficker, and myDoom—to name a few. The security community has evolved and grown smarter about security, safe computing, and system hardening but so have our adversaries. This decade is setting up to be the exponential jumping off point. The adversaries are rapidly leveraging productized malware toolkits that let them develop more malware than in all prior years combined, and they have matured from the prior decade to release the most insidious and persistent cyberthreats ever known.

The Google hacks ("Operation Aurora"), named by McAfee and announced in January 2010, and the WikiLeaks document disclosures of 2010 have highlighted the fact that external and internal threats are nearly impossible to prevent. Miscreants continue to infiltrate networks and exfiltrate sensitive and proprietary data upon which the world's economies depend every day. When a new attack emerges, security vendors cannot stand by idly and watch. We are obligated to share our findings to protect those not yet impacted and to repair those who have been. As such, McAfee Foundstone Professional Services and McAfee Labs decided to release the following discovery.

Starting in November 2009, coordinated covert and targeted cyberattacks have been conducted against global oil, energy, and petrochemical companies. These attacks have involved 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. We have identified the tools, techniques, and network activities used in these continuing attacks—which we have dubbed Night Dragon—as originating primarily in China. Through coordinated analysis of the related events and tools used, McAfee has determined identifying features to assist companies with detection and investigation. While we believe many actors have participated in these attacks, we have been able to identify one individual who has provided the crucial C&C infrastructure to the attackers. *(See Appendix B for more detail on attribution.)*

Anatomy of a Hack

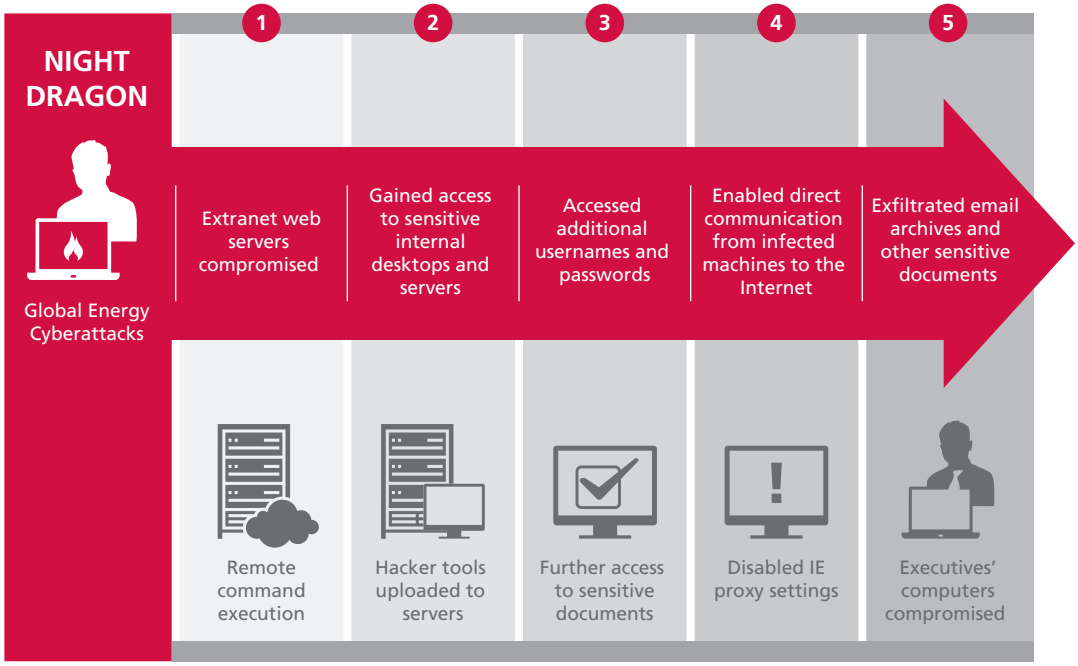


Figure 1. Anatomy of a hack.

The Night Dragon attacks work by methodical and progressive intrusions into the targeted infrastructure. The following basic activities were performed by the Night Dragon operation:

- Company extranet web servers compromised through SQL-injection techniques, allowing remote command execution
- Commonly available hacker tools are uploaded on compromised web servers, allowing attackers to pivot into the company's intranet and giving them access to sensitive desktops and servers internally
- Using password cracking and pass-the-hash tools, attackers gain additional usernames and passwords, allowing them to obtain further authenticated access to sensitive internal desktops and servers
- Initially using the company's compromised web servers as command and control (C&C) servers, the attackers discovered that they needed only to disable Microsoft Internet Explorer (IE) proxy settings to allow direct communication from infected machines to the Internet
- Using the RAT malware, they proceeded to connect to other machines (targeting executives) and exfiltrating email archives and other sensitive documents

Details of the Attack

Attackers using several locations in China have leveraged C&C servers on purchased hosted services in the United States and compromised servers in the Netherlands to wage attacks against global oil, gas, and petrochemical companies, as well as individuals and executives in Kazakhstan, Taiwan, Greece, and the United States to acquire proprietary and highly confidential information. The primary operational technique used by the attackers comprised a variety of hacker tools, including privately developed and customized RAT tools that provided complete remote administration capabilities to the attacker. RATs provide functions similar to Citrix or Microsoft Windows Terminal Services, allowing a remote individual to completely control the affected system.

To deploy these tools, attackers first compromised perimeter security controls, through SQL-injection exploits of extranet web servers, as well as targeted spear-phishing attacks of mobile worker laptops, and compromising corporate VPN accounts to penetrate the targeted company's defensive architectures (DMZs and firewalls) and conduct reconnaissance of targeted companies' networked computers.

SQL Injection Attacks

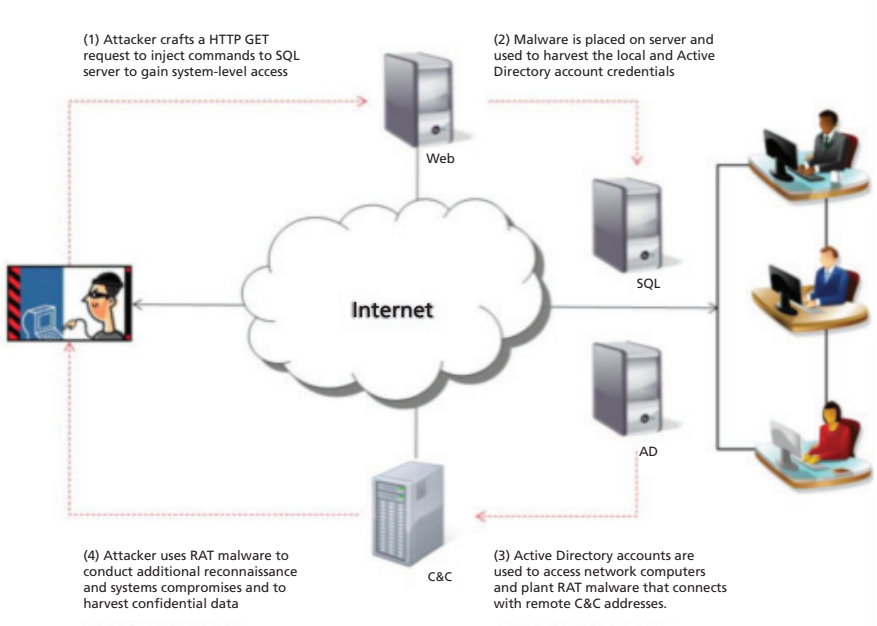


Figure 2. SQL-injection attacks.

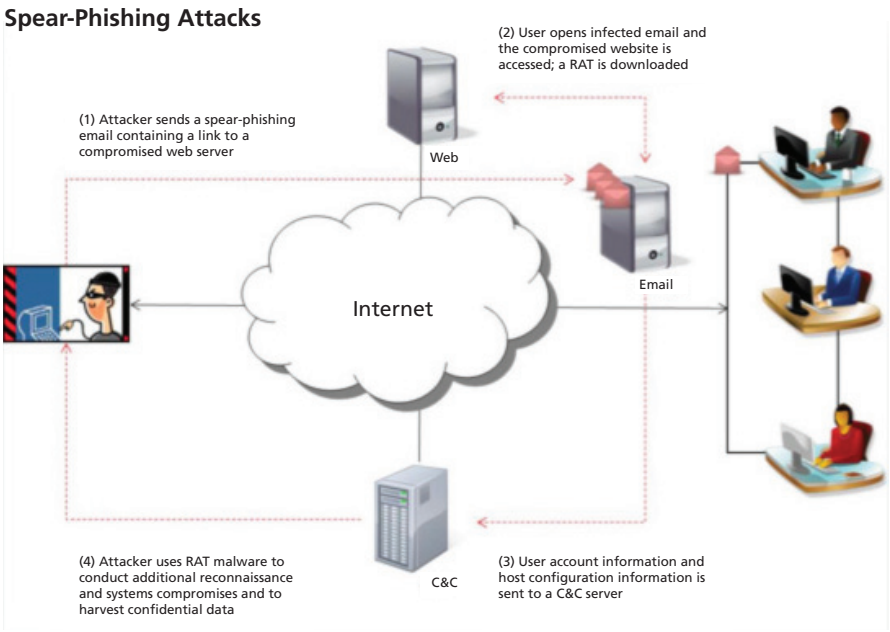


Figure 3. Spear-phishing attacks.

Many Chinese hacker websites offer these tools for download, including links to reduh, WebShell, ASPXSpy, and many others, plus exploits and zero-day malware.

Figure 4. Rootkin.net.cn offers access to an endless list of hacker tools and exploits.

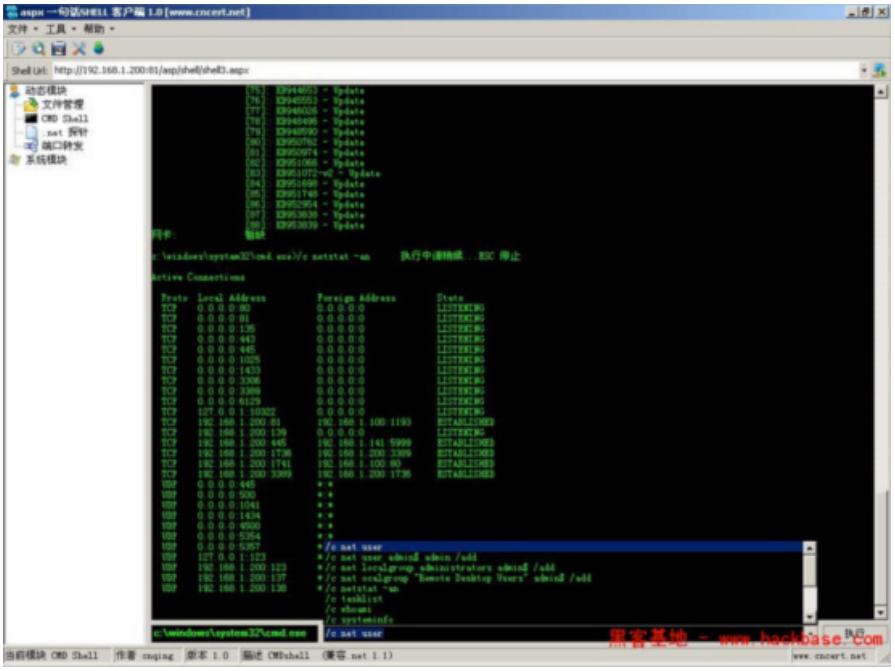


Figure 5. WebShell and ASPXSpy tools allow an attacker to bypass many firewall rules to funnel all control through a company’s web server.

Once the initial system was compromised, the attackers compromised local administrator accounts and Active Directory administrator (and administrative users) accounts. The attackers often used common Windows utilities, such as SysInternals tools (acquired by Microsoft in 2006)—and other publicly available software, including hacking tools developed in China and widely available on Chinese underground hacker websites—to establish "backdoors" through reverse proxies and planted Trojans that allowed the attackers to bypass network and host security policies and settings. Desktop anti-virus and anti-spyware tools were also disabled in some instances—a common technique of targeted attacks.

Use of remote administration tools

Remote administration tools (RATs) are commonly used administrative tools that allow hackers (and administrators) to manage victims' computers (or managed systems) and completely control their use and function. A commonly used RAT in the hacker community is Gh0st and its many variants. RAT features often include screen and webcam spying, keystroke logging, mouse control, file/registry, and process management, and, of course, remote command shell capability.

McAfee has identified several RATs that have been used to establish a persistent infiltration channel into compromised companies. One of the most prevalent RATs is zwShell, which McAfee has seen in the wild since the spring of 2010 (compiled on 2010-03-17 08:47:00). Written in the Delphi language, zwShell was used by attackers to both build custom variants of the Trojan that they deployed on dozens of machines within each victim company, as well as to control compromised machines that would initiate beacon connections to it on a custom protocol.

Attackers used zwShell extensively to generate dozens of unique Trojan variants and to control the infected machines and exfiltrate sensitive data directly from them. (See Appendix A for a breakdown of the zwShell.)

Once the attackers had complete control of the targeted internal system, they dumped account hashes with gsecdump and used the Cain & Abel tool to crack the hashes to leverage them in targeting ever more sensitive infrastructures.

Files of interest focused on operational oil and gas field production systems and financial documents related to field exploration and bidding that were later copied from the compromised hosts or via extranet servers. 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.

Detection

The methods and tools used in these attacks are relatively unsophisticated, as they simply appear to be standard host administration techniques, using standard administrative credentials. This is largely why they are able to evade detection by standard security software and network policies. Since the initial compromises, however, many individual unique signatures have been identified for the Trojan and associated tools by security vendors, including McAfee; yet only through recent analysis and the discovery of common artifacts and evidence correlation have we been able to determine that a dedicated effort has been ongoing for at least two years, and likely as many as four. We can now associate the various signatures to these events.

The following artifacts can help to determine whether a company has been compromised:

- Host files and/or registry keys
- Anti-virus alerts
- Network communications

Host Files and Registry Keys

Utility	Description
Command & control application	zwShell.exe 093640a69c8eafbc60343bf9cd1d3ad3 zwShell.exe 85df6b3e2c1a4c6ce20fc8080e0b53e9
Trojan dropper	A packaged executable customized to each victim that includes the 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 or programs, such as "Event Log Explorer" or EnCase, which support search capabilities. When executed, the dropper creates a temporary file that is reflected in Windows update logs (KB*.log files in c:\Windows folder). This is because the Windows Registry is modified by the dropper to create a "netsvcs" key. Accordingly, the date of the backdoor installation can be determined from a search of the KB log files. This temporary file is also identified in the backdoor DLL itself. The temporary file is usually some alphanumeric combination that includes "gzg" (for example, xgt0gzg); however, it has been seen with generic file names (for example, server.exe) as well. 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 unless it uses a different configuration.
Trojan backdoor	Dynamic link libraries (DLLs), also appearing 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 Initially configured with the following: connect.dll 6E31CCA77255F9CDE228A2DB9E2A3855 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.

*This DLL uses a different C&C application that may be an earlier version of zwShell, analysis continues.

The Trojan components are manually copied or delivered through administrative utilities to remote systems. They do not include any worm or self-replicating features, nor can the Trojan "infect" other computers. Removing the Trojan components is simply a matter of deleting the related files and registry settings.

The Trojan backdoor communicates with the C&C server at the address hard-coded in each DLL. The C&C server cannot modify the backdoor once it is installed; related systems must have the Trojan file removed before a new backdoor DLL can be installed on the system. Thus, if the C&C server address is changed, those servers that have the DLL with previous addresses must be remotely administered by the attacker.

Anti-virus Alerts

Anti-virus patterns are defined according to samples submitted by clients or analysts as they are discovered. Some Trojans exhibit characteristics of other types of malware, such as worms or viruses, that have the ability to infect other systems. RATs do not typically include such features, and, because they are defined with unique configurations for custom purposes, they commonly change faster than unique samples can be identified.

Only when an entire RAT toolkit is found can we define an anti-virus pattern that is generic enough to detect the RAT regardless of configuration changes. The package necessarily includes the C&C application server, the generator utility for creating droppers, related droppers, and backdoors—and a sufficient number of each to correlate the toolkit.

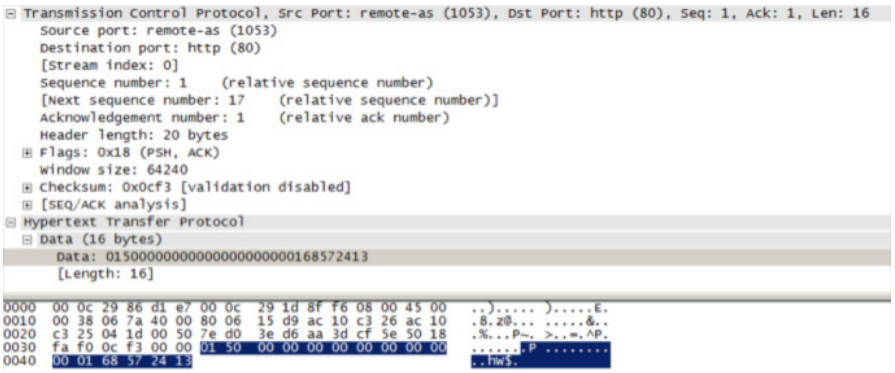
As mentioned previously, there have been several unique patterns developed from samples submitted to McAfee (as well as to other anti-virus vendors).

McAfee recommends that companies review McAfee ePolicy Orchestrator® (McAfee ePO™) software and anti-virus logs for "NightDragon" signature detections to identify related alerts since 2007 and then recover and resubmit these samples for analysis to investigate the related incidents. McAfee can assist with the analysis or provide instructions and tools for internal review.

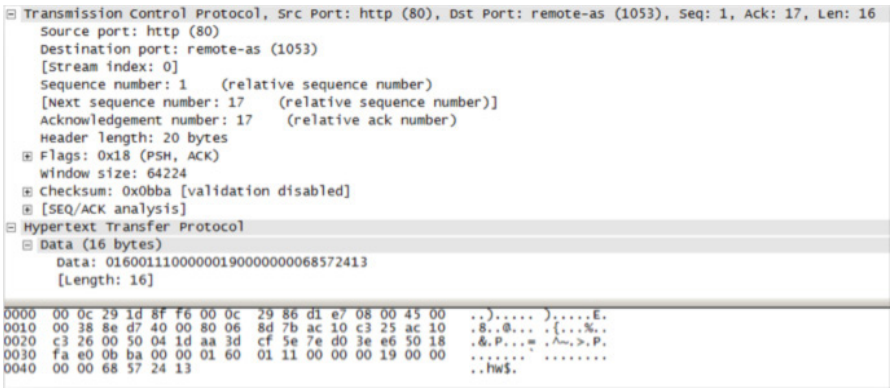
Network Communications

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 0x42 within the TCP packet.

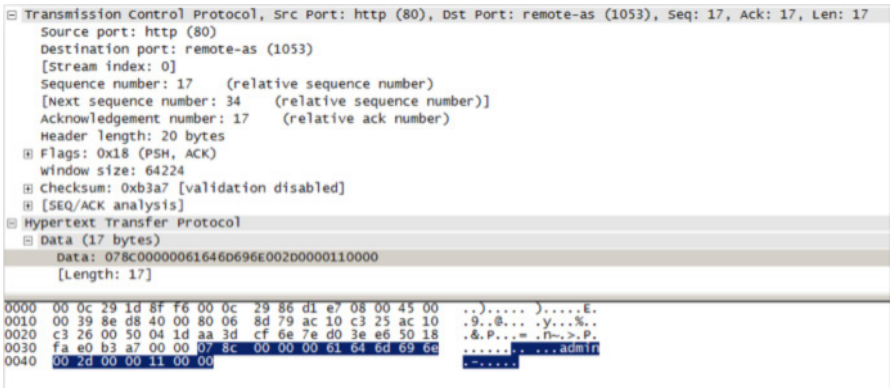
The backdoor begins its beacon at approximately five-second intervals with an initial packet that may be detected with the pattern: "\x01\x50[\x00-\xff]+\x68\x57\x24\x13."



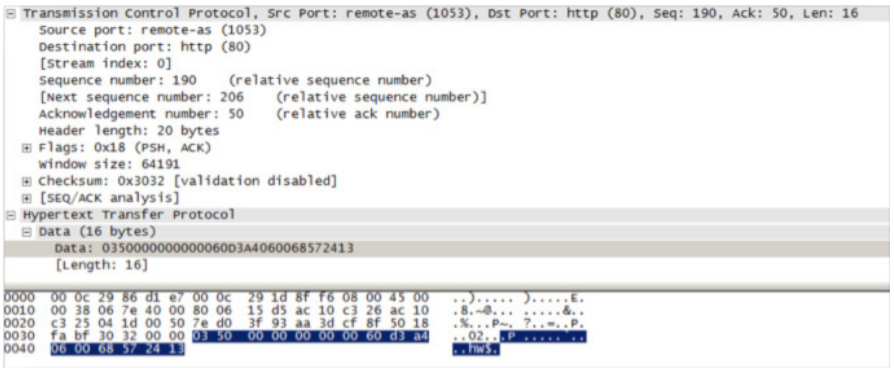
The server acknowledges the beacon with an initial response of "\x01\x60[\x00-\xff]+\x68\x57\x24\x13."



The backdoor sends the password to the server in clear text after the server acknowledges the connection.



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."



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):

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

Note: The above hostnames (is-a-chef.com<http://is-a-chef.com>, thruhere.net<http://thruhere.net>, office-on-the.net<http://office-on-the.net>, selfip.com<http://selfip.com>) by themselves do not indicate malicious activity and there are plenty of legitimate subdomains that may use those hostnames. Communication to those hostnames should be carefully scrutinized but not necessarily raise alarm on its own

Company extranet servers have also been used as either unique or secondary/redundant C&C servers. In some instances, the attackers have (probably mistakenly) used droppers configured to compromise one company's computers—in another company's computers.

McAfee recommends that companies configure intrusion detection system (IDS) rules to detect the noted signatures (or employ the user-defined signature [UDS] "BACKDOOR: NightDragon Communication Detected" in McAfee Network Security Platform) and monitor DNS for outbound communications to dynamic DNS addresses resolving to or pathed back as suballocated to servers in China, where the company's name or common abbreviation forms the first part of the address. This may be difficult. However, if samples of the backdoor DLLs are found, DNS monitoring can help to identify other compromised hosts in the company network. McAfee also recommends that companies review web or IDS logs for file transfers to addresses registered in China. McAfee can assist with the analysis or provide instructions and tools for internal review.

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. Anti-virus may or may not detect the Trojan unless it is beaconing or a full file system scan is performed.

McAfee Early Detection

Customers can deploy a number of McAfee products to help protect information systems from the Night Dragon attack:

- *McAfee Vulnerability Manager:* Using agentless discovery and vulnerability checking to assess systems on your network, McAfee Vulnerability Manager is an enterprise-class vulnerability management system that will detect infected Night Dragon systems as well as the security weaknesses in systems that have been compromised. The "wham-apt-nightdragon-detected-v7.fasl3" script will detect this threat remotely on systems.

- *McAfee Policy Auditor:* Using agent-based configuration audit checks to determine the most secure configuration of a system, McAfee Policy Auditor software detects the security weaknesses in the systems that have been compromised
- *McAfee Risk Advisory (MRA):* Properly deployed, McAfee Risk Advisor would have allowed administrators to see the misconfigurations and gap in security coverage that facilitated Night Dragon's exploitation

McAfee Detection

Night Dragon also displays a pattern of correlated activities with an assortment of other software tools that McAfee can assist companies to identify.

- *McAfee VirusScan Enterprise:* Update your anti-virus .DATs to at least version 6232 and ensure that on-demand scans are working properly and perform a full file system virus scan. Review McAfee ePO software or anti-virus alerts and network logs for "NightDragon" signature detections to identify compromised systems. Please submit any related samples to virus_research@mcafee.com or submit on the web at https://www.webimmune.net/default.asp.
- *McAfee Network Threat Response:* McAfee Network Threat Response technology would have detected the malicious C&C traffic and would have alerted administrators to the attack early, giving them time to react and prevent future damage

Administrators can also download the following free tools from McAfee:

- McAfee "Night Dragon Vulnerability Scanner" based on McAfee Vulnerability Manager technology to scan their networks for the presence of malware
- McAfee Labs Stinger

McAfee Prevention

For complete prevention of this and most other attacks involving advanced persistent threats (APTs), customers can deploy application whitelisting and change/configuration control software on their critical servers. These technologies completely prevent the unauthorized running of DLLs/EXEs as well as the modification of registry keys, services, and more involved in all of today's APT and zero-day attacks.

- *McAfee Application Control:* McAfee Application Control software stops Night Dragon by not allowing the dropper files from executing (even as administrator on Windows), thereby preventing downloads of additional malware and the setup of C&C channels that allowing RAT control and theft of sensitive files
- *McAfee Configuration Control:* McAfee Configuration Control software allows you to disallow any configuration changes to your systems, protecting them from being modified without explicit permission (even with administrative access)
- *McAfee Database Activity Monitoring:* delivers complete database protection including 0-day attacks and web born attacks such as those seen with SQL injection in Night Dragon.
- *McAfee Network Security Platform:* blocks malicious network activity such as APT command and control traffic.
- *McAfee Enterprise Firewall:* Properly installed and configured at the border and inside your organization, McAfee Firewall would have prevented the Night Dragon operation from penetrating so deeply into the affected organizations and would have blocked C&C communication from the RAT
- *McAfee Web Gateway:* Properly installed and configured, McAfee Web Gateway would have prevented the Night Dragon operation from using their RATs, requiring them to proxy-enable their RATs or use alternative proxy-enabled RATs
- *McAfee Endpoint Encryption:* Properly installed and configured, McAfee Endpoint Encryption software reduces the impact of the Night Dragon attack by restricting access to the core targeted assets

- *McAfee Data Loss Protection:* Properly installed and configured, McAfee Network DLP and/or McAfee Host DLP solutions allow you to prevent and detect the extraction of sensitive information from outside the company
- *McAfee Host Intrusion Prevention 8.0:* McAfee Host Intrusion Prevention 8.0 software has introduced a new "TrustedSource" APT detection feature that allows enterprises to correlate endpoint executable activity with the network C&C communication to detect and prevent RAT communications and data exfiltration activity
- *McAfee VirusScan® Enterprise:* In addition to detecting associated malware and RATs on the endpoint, customers can also leverage access protection features in McAfee VirusScan Enterprise to prevent (and alert on) the creation of Night Dragon-related files and folder structures. Other built-in features such infection tracing and McAfee Global Threat Intelligence™ can assist with the identification and quarantining or removal of new and unknown associated malware and RATs.

If you have discovered the presence of Night Dragon in your environment and would like incident-response or forensics assistance to respond and repair, please contact Foundstone Professional Services on incidentresponse@foundstone.com or submit any related samples to Virus_Research@avertlabs.com or on the web at McAfee Labs WebImmune.

Conclusion

Well-coordinated, targeted attacks such as Night Dragon, orchestrated by a growing group of malicious attackers committed to their targets, are rapidly on the rise. These targets have now moved beyond the defense industrial base, government, and military computers to include global corporate and commercial targets. While Night Dragon attacks focused specifically on the energy sector, the tools and techniques of this kind can be highly successful when targeting any industry. Our experience has shown that many other industries are currently vulnerable and are under continuous and persistent cyberespionage attacks of this type. More and more, these attacks focus not on using and abusing machines within the organizations being compromised, but rather on the theft of specific data and intellectual property. It is vital that organizations work proactively toward protecting the heart of their value: intellectual property. Enterprises need to take action to discover these assets in their environments, assess their configurations for vulnerabilities, and protect them from misuse and attack.

For additional research and information, review *Hacking Exposed: Network Secret and Solutions—6th Edition* (Osborne McGraw-Hill). You can also visit http://www.hackingexposed.com for information on advanced hacker techniques and to sign up for "Hacking Exposed" monthly webinars.

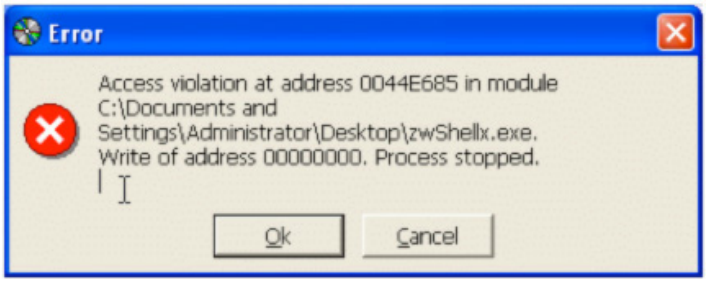
Credits and Acknowledgements

The preceding white paper was a collaborative effort among numerous people and entities including McAfee Foundstone Professional Services consultants, McAfee Labs, McAfee employees, executives, and researchers, HBGary and National Cyber-Forensics & Training Alliance (NCFTA). Significant contributors include Shane Shook, Dmitri Alperovitch, Stuart McClure, Georg Wicherski, Greg Hoglund, Shawn Bracken, Ryan Permeh, Vitaly Zaytsev, Mark Gilbert, Mike Spohn, George Kurtz, and Adam Meyers.

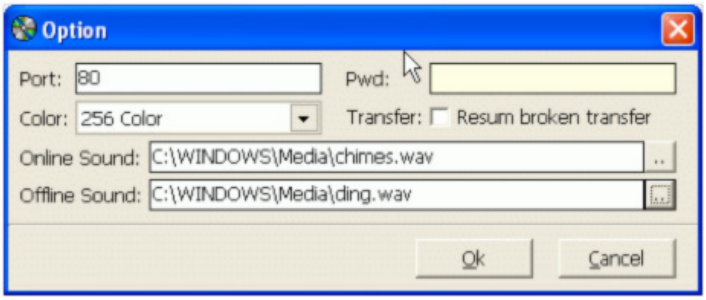
Appendix A: zwShell—the RAT

Below is a walk-through of the capabilities of zwShell and a demonstration of how the attackers used zwShell as a command and control server to exfiltrate data from within the targeted companies.

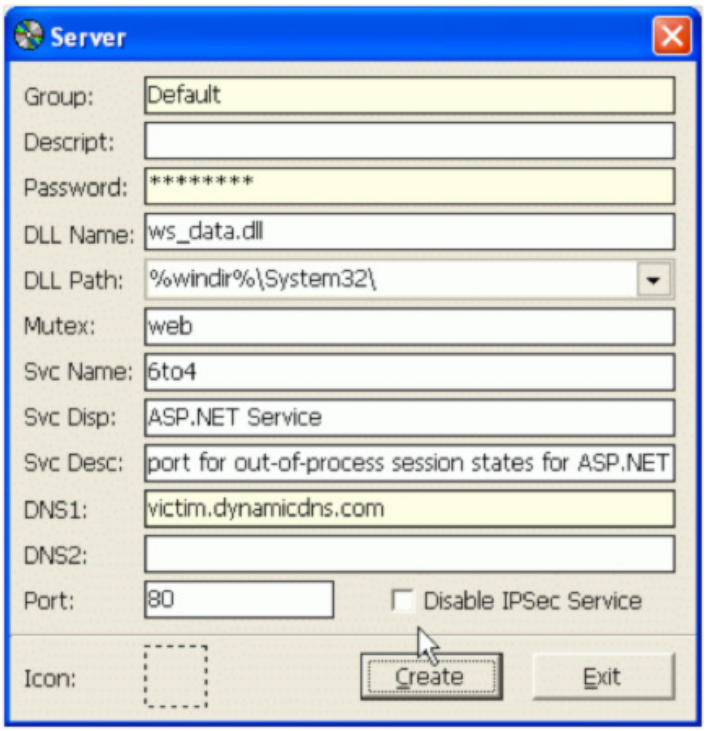
1. When zwShell is launched, it presents a fake crash error to the user and contains a hidden text entry field below the "Write of address 00000000. Process stopped" line. By entering the password in the hidden dialog box above the "ok" button to launch the application requires typing a special password, "zw.china." Without that password, the tool will not start. This obfuscation method is likely used to confuse investigators about the true purpose of this executable.



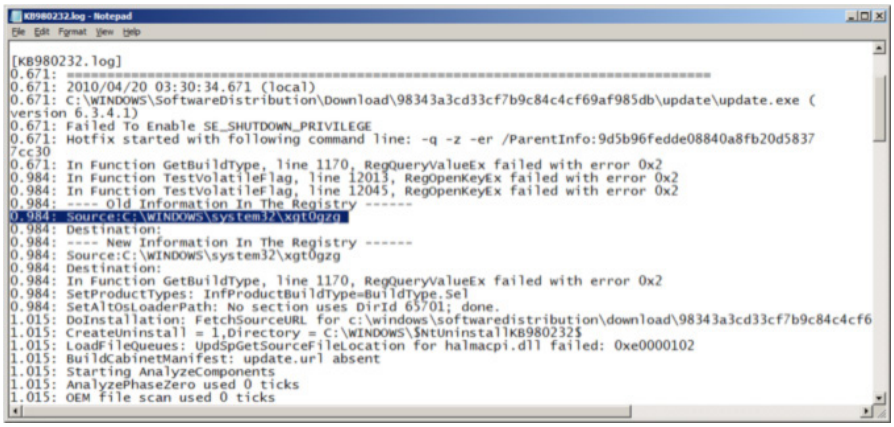
2. Once the error is bypassed, and zwShell is launched, it allows the attacker to create a custom Trojan by selecting the Server menu or to launch the C&C server by clicking Start and entering the port to listen for traffic with the password used by the backdoor DLLs. Once started, the application will begin listening for incoming compromised client connections and display them inside the grid. The attacker can launch as many instances of the zwShell application as required—as long as each listens to a different port or password. In this manner, multiple "networks" of compromised computers can be monitored.
3. The attacker can also click on the Options menu to configure the C&C server settings. Those settings include selection of the listening port, the password that will encrypt the C&C traffic (which must match the password selected at the time of the Trojan generation), the ability to specify custom sound notifications for when infected machines connect and disconnect from the C&C server, and the ability to increase the color depth used for remote access to the machine, as well as an optional capability to allow resumes of interrupted file transfers from the client machine. The attacker can stop the listener and start with new options to monitor or connect with other compromised computers.



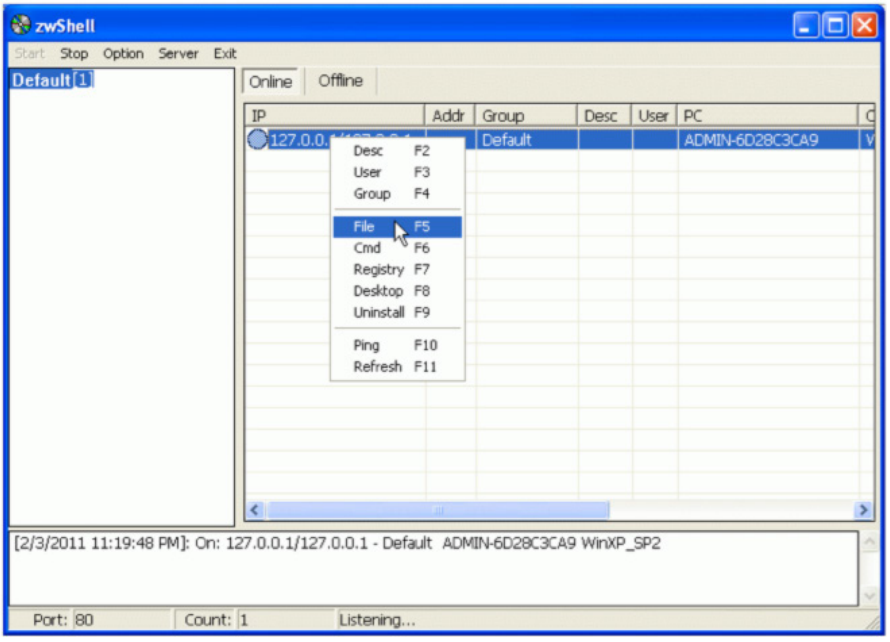
4. The attacker can specify the password (which must match the password set up for the server in Step 3), the name and path to the RAT DLL that will be injected into the svchost.exe Windows services process, the service and mutex names, and service displayed name and description. The attacker can also specify up to two C&C hostnames or IP address, port address, and dropper EXE process icon. Once the Create button is clicked, zwShell will generate a custom EXE dropper process which, when executed, will delete itself and extract a RAT DLL that will be launched as a persistent Windows service. The RAT will then immediately send a beacon on the configured port to the designated C&C server and wait for instructions.



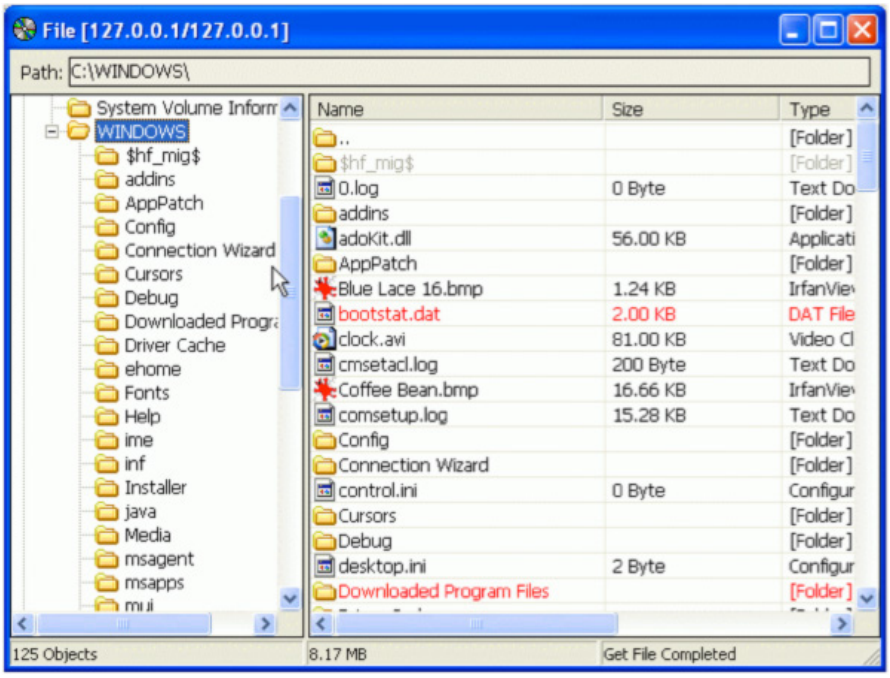
5. The dropper will be copied over network shares to the compromised computer and remotely execute with psexec or via Windows Terminal Services (RDP). In some cases, an "AT.job" or "SchTasks" entry will be used to execute the dropper over the network on the compromised computer. When executed, the dropper will create a temporary file and extract a RAT DLL that will be launched as a persistent Windows service. The RAT will then immediately send a beacon on the configured port to the designated C&C server and wait for instructions. The dropper will automatically delete itself after the backdoor service is created, and the temporary file will be deleted when the system is rebooted. An entry will be created in the Windows Update logs (KB****.log) in the C:\Windows directory with the date and time and path+name of the temporary file.



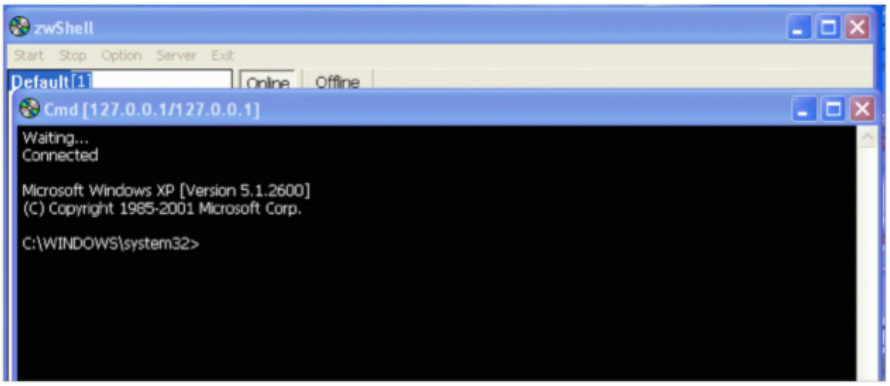
6. When a client is executed, it connects to the attacker's zwShell interface, along with its IP address, PC name, name of the logged-in user, and information about the operating system (OS) version of the machine, including the major patch levels.
7. The attacker in charge of the C&C server can establish full remote control of the connected machine and can browse the file system, launch command-line shells, manipulate the registry, view the remote desktop, and uninstall the Trojan from the client.



8. Browsing the client file system is a fully interactive process and has a familiar user interface similar to Windows Explorer. Individual files and folders can be deleted, renamed, copied, downloaded, and uploaded to the remote machine.



9. A remote command-line shell can be launched to execute commands directly on the remote machine. When the attacker uses this function, a copy of CMD.EXE is copied to the compromised system in a Windows %Temp% directory with the filename svchost.exe. This copy is an unmodified version of the Microsoft Windows command shell executable.



10. The Registry can also be viewed and edited in a user interface similar to the Windows Registry editor.

Appendix B: Attribution

IMPORTANT: McAfee has no direct evidence to name the originators of these attacks but rather has provided circumstantial evidence.

While we believe many actors have participated in these attacks, we have been able to identify one individual who has provided the crucial C&C infrastructure to the attackers—this individual is based in Heze City, Shandong Province, China. Although we don't believe this individual is the mastermind behind these attacks, it is likely this person is aware or has information that can help identify at least some of the individuals, groups, or organizations responsible for these intrusions.

Figure 6. Shandong Province, China

The individual runs a company that, according to the company's advertisements, provides "Hosted Servers in the U.S. with no records kept" for as little as 68 RMB (US$10) per year for 100 MB of space. The company's U.S.-based leased servers have been used to host the zwShell C&C application that controlled machines across the victim companies.

Beyond the connection to the hosting services reseller operation, there is other evidence indicating that the attackers were of Chinese origin. Beyond the curious use of the "zw.china" password that unlocks the operation of the zwShell C&C Trojan, McAfee has determined that all of the identified data exfiltration activity occurred from Beijing-based IP addresses and operated inside the victim companies weekdays from 9:00 a.m. to 5:00 p.m. Beijing time, which also suggests that the involved individuals were "company men" working on a regular job, rather than freelance or unprofessional hackers. In addition, the attackers employed hacking tools of Chinese origin and that are prevalent on Chinese underground hacking forums. These included Hookmsgina and WinlogonHack, tools that intercept Windows logon requests and hijack usernames and passwords.

```
WinlogonHack

一。执行install.bat 安装。
      不用重启，当有3389登上时，自动加载DLL，并且记录登录密码！ 保存为boot.dat文件.

二。运行ReadLog.bat 移动密码文件到当前目录。查看吧~

三。执行Uninstall.bat，若 %systemroot%\system32\wminotify.dll 文件未能删除，那就重启再删了吧，润物细无声~~~

没测试过windows 2000，有条件测试的朋友测试一下，告诉我一声！ 谢谢

QQ:343789385

www.lovemfc.cn
```

Figure 7. Instructions on the use of WinlogonHack tool by its Chinese developers.

On the compromised web server, they also deployed ASPXSpy, a web-based remote administration tool, also of Chinese origin.

```
<%@ Assembly Name="System.DirectoryServices,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
<%@ Assembly Name="System.Management,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
<%@ Assembly Name="System.ServiceProcess,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
<%@ Assembly Name="Microsoft.VisualBasic,Version=7.0.3300.0,Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<script runat="server">
/*
Thanks Snailsor,FuYu,BloodSword,Cnqing,
Code by Bin
Make in China
Blog: http://www.rootkit.net.cn
E-mail : master@rootkit.net.cn
*/
public string Password="191d0b796a16ed11a2a58aa14fdb0112";//admin
public string vbhLn="ASPXSpy";
public int TdgGU=1;
protected OleDbConnection Dtdr=new OleDbConnection();
protected OleDbCommand Kkvb=new OleDbCommand();
```

Figure 8. Parts of the ASPXSpy code with attribution to the Chinese developer.

There is nothing to suggest that the developers of these tools had any direct connection to these intrusions, as the tools are widely available on the Chinese web forums and tend to be used extensively by Chinese hacker groups. Although it is possible that all of these indicators are an elaborate red-herring operation designed to pin the blame for the attacks on Chinese hackers, we believe this to be highly unlikely. Further, it is unclear who would have the motivation to go to these extraordinary lengths to place the blame for these attacks on someone else. We have strong evidence suggesting that the attackers were based in China.

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

21401wp_night-dragon_0211