

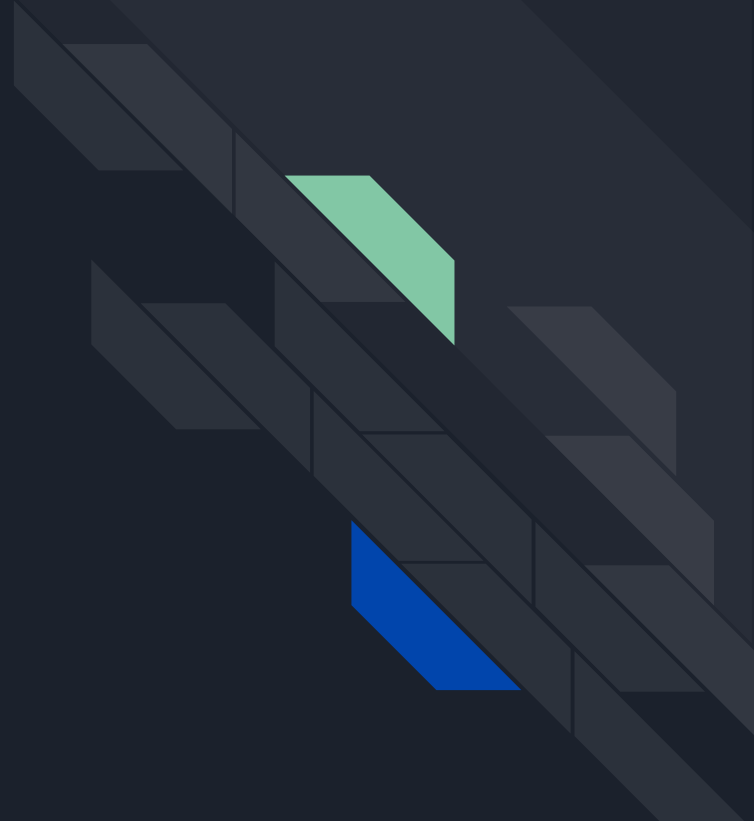


Night Dragon

Namrha Chohan, Tanya Malik, Mohammad H Asim,
Ruiqi Cui, Nikshipta Koya, Maisha Tabassum, and
Hemanth Jampani

Agenda

- Problem Statement
- Night Dragon
- Actors and Motivation
- Pros/cons
- Lessons learned





Problem Statement

- Night Dragon targeted energy companies with sophisticated and coordinated campaign
 - Compromised sensitive information
 - Disrupted operations
 - Potentially gained unauthorized access to critical infrastructure
- Attackers employed various methods
 - APTs
 - Malware
 - Social engineering techniques to exploit vulnerabilities in target organizations' networks



Affected Users/why do we care?

- Targeted 71 organizations, mostly in the energy sector, in mid-2006
 - One of the first attacks targeting the energy sector
 - Attacked Government and military computers
- Headlines until 2011 by Dmitri Alperovitch, vice president of threat research at cybersecurity company McAfee
- Awareness



Night Dragon - what is it?

GOAL: Attain executive confidential information from energy sector companies.

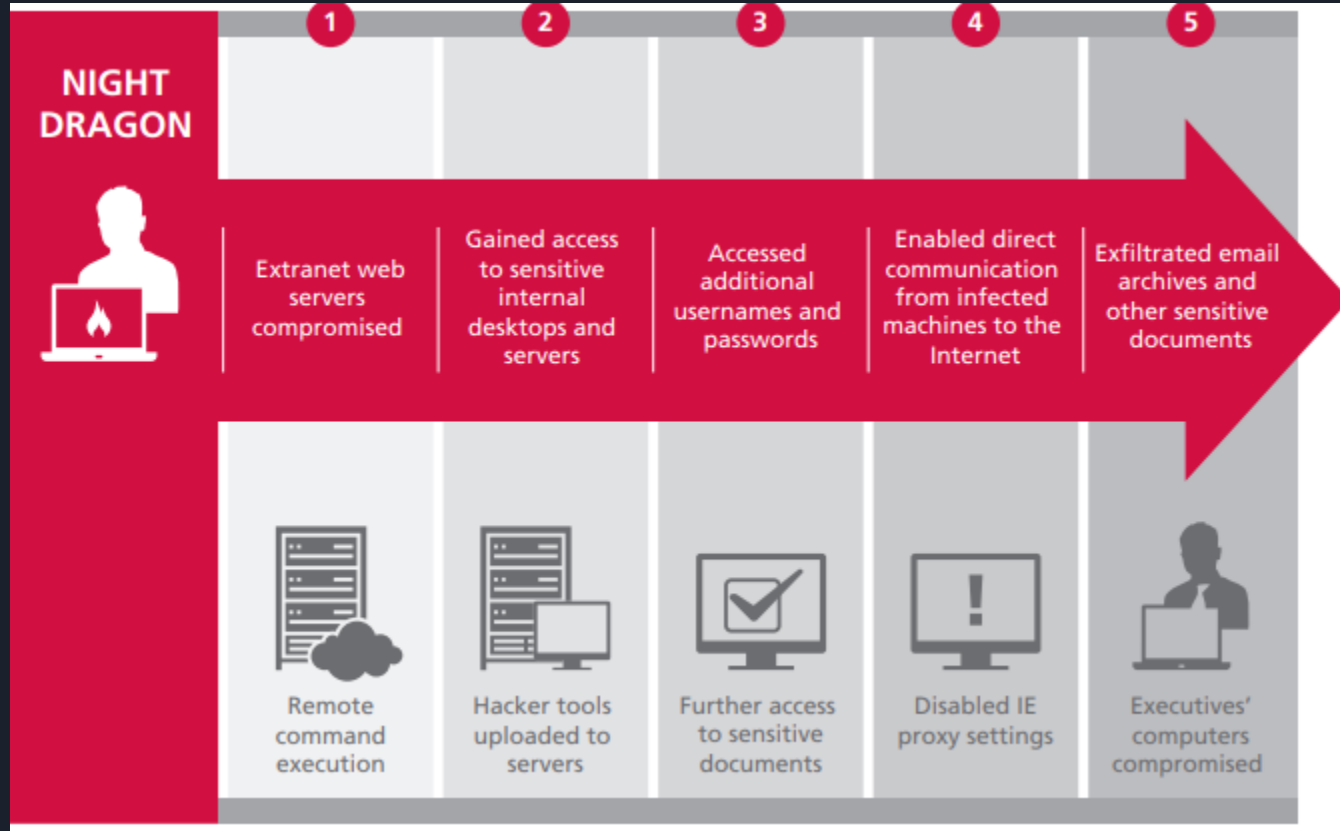
- Sensitive information competitors
- Project financing information on oil and gas fields
- Project bids and operations



Night Dragon - how was it done?

- Trojan backdoor - no self propagation
- Installed on different computers using .exe on windows share
 - Social Engineering
 - Trojan
 - RAT
 - Spear phishing
 - Vulnerability exploits in the windows OS
 - AD compromises

Attack Sequence



Actors and Motivation

01 Identified an individual from Shandong, China with confirmed links to the cyber attack.

02 Traced the attack's timezone and originating IP addresses to Beijing.

03 Investigated cases of industrial espionage within the oil and gas sector.

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.lovmfc.cn

```
<%@ 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 Snailor,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();
```




Kill Chain

- 01 Comprised the perimeter controls and penetrated into the internal network
- 02 Uploaded freely available hacker tools in the compromised servers
- 03 Infected machines with Remote Administration Trojans
- 04 Once the attackers had complete control of the targeted internal system they dumped account hashes and cracked them to get even more sensitive data



Detection

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

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



Host files and/or registry keys :

- The Trojan components are manually copied or delivered through administrative utilities to remote systems.
- The communication between the C&C server and the DLLs occurs at a specific address hardcoded in the DLL

Anti-Virus Alerts :

- Only when a RAT toolkit is found we can define an anti-virus pattern , As RATs typically doesn't include features of worms or ability to multiply and infect other systems
- Signatures or patterns can be generated based on the samples submitted and many unique patterns has been developed.

Network Communication :

- 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.”
- 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.”
- As the attackers use dynamic DNS name service accounts, The commonly used C&C traffic include is-a-chef.com, thruhere.net, office-on-the.net and selfip.com.



Consequences

1. Targeted Attacks
2. Data Theft
3. Financial Damage
4. Reputational Damage
5. Increased Awareness



Lesson Learned in Cybersecurity

Targeted Industry Risks:

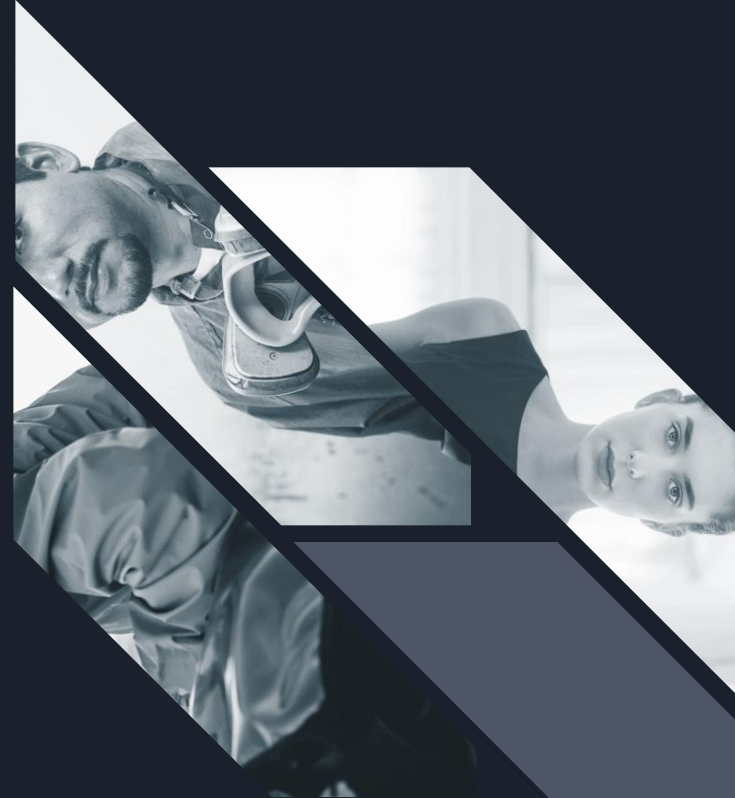
- Cyber threats may exploit vulnerabilities unique to specific industries.
- Organizations need to be aware of industry-specific risks and tailor security measures accordingly.


Persistent Advanced Threats:

- Advanced persistent threats (APTs) can persist for extended periods.
- Continuous monitoring, threat intelligence sharing, and robust incident response plans are crucial.

Social Engineering and Spear-Phishing:

- Initial access often occurs through social engineering and spear-phishing.
- Employee training on recognizing phishing attempts is essential.





Lesson Learned in Cybersecurity Continued

Software Vulnerability Management:

- Cyber attackers exploit software vulnerabilities.
- Regularly applying patches and updates is crucial to minimize the risk of exploitation.

Access Controls and Credential Management:

- Compromising Active Directory provides significant access.
- Implementing strong access controls, monitoring, and multi-factor authentication is critical.

Incident Response and Monitoring:

- Well-defined incident response plans are essential.
- Continuous monitoring, auditing, and collaboration with cybersecurity organizations enhance threat detection and response.



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



Thank you!

Q&A

