Symantec™
Security Response

The Nitro Attacks

Stealing Secrets from the Chemical Industry

Eric Chien and
Gavin O’Gorman

Contents

Introduction

This document discusses a recent targeted attack campaign directed primarily at private companies involved in the research, development, and manufacture of chemicals and advanced materials. The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes. In addition, the same attackers appear to have a lengthy operation history including attacks on other industries and organizations. Attacks on the chemical industry are merely their latest attack wave. As part of our investigations, we were also able to identify and contact one of the attackers to try and gain insights into the motivations behind these attacks. As the pattern of chemical industry targets emerged, we internally code-named the attack campaign Nitro.

The attack wave started in late July 2011 and continued into mid-September 2011. However, artifacts of the attack wave such as Command and Control (C&C) servers are also used as early as April 2011 and against targets outside the chemical industry. The purpose of the attacks appears to be industrial espionage, collecting intellectual property for competitive advantage.

Targets

The attackers have changed their targets over time. From late April to early May, the attackers focused on human rights related NGOs. They then moved on to the motor industry in late May. From June until mid-July no activity was detected. At this point, the current attack campaign against the chemical industry began. This particular attack has lasted much longer than previous attacks, spanning two and a half months.

A total of 29 companies in the chemical sector were confirmed to be targeted in this attack wave and another 19 in various other sectors, primarily the defense sector, were seen to be affected as well. These 48 companies are the minimum number of companies targeted and likely other companies were also targeted. In a recent two week period, 101 unique IP addresses contacted a command and control server with traffic consistent with an infected machine. These IPs represented 52 different unique Internet Service Providers or organizations in 20 countries.

Companies affected include:

- Multiple Fortune 100 companies involved in research and development of chemical compounds and advanced materials.
- Companies that develop advanced materials primarily for military vehicles.
- Companies involved in developing manufacturing infrastructure for the chemical and advanced materials industry.

Attack methodology

The attackers first researched desired targets and then sent an email specifically to the target. Each organization typically only saw a handful of employees at the receiving end of these emails. However, in one organization almost 500 recipients received a mail, while in two other organizations, more than 100 were selected. While the attackers used different pretexts when sending these malicious emails, two methodologies stood out. First, when a specific recipient was targeted, the mails often purported to be meeting invitations from established business partners. Secondly, when the emails were being sent to a broad set of recipients, the mails purported to be a necessary security update. The emails then contained an attachment that was either an executable that appeared to be a text file based on the file name and icon, or a password-protected archive containing an executable file with the password provided in the email. In both cases, the executable file was a self-extracting executable containing PoisonIvy, a common backdoor Trojan developed by a Chinese speaker.

When the recipient attempted to open the attachment, they would inadvertently execute the file, causing PoisonIvy to be installed. Once PoisonIvy was installed, it contacted a C&C server on TCP port 80 using an encrypted communication protocol. Using the C&C server, the attackers then instructed the compromised computer to provide the infected computer's IP address, the names of all other computers in the workgroup or domain, and dumps of Windows cached password hashes.

By using access to additional computers through the currently logged on user or cracked passwords through dumped hashes, the attackers then began traversing the network infecting additional computers. Typically, their primary goal is to obtain domain administrator credentials and/or gain access to a system storing intellectual property. Domain administrator credentials make it easier for the attacker to find servers hosting the desired intellectual property and gain access to the sensitive materials. The attackers may have also downloaded and installed additional tools to penetrate the network further.

While the behavior of the attackers differs slightly in each compromise, generally once the attackers have identified the desired intellectual property, they copy the content to archives on internal systems they use as internal staging servers. This content is then uploaded to a remote site outside of the compromised organization completing the attack.

Geographic Spread

Figure 1 shows the location of infected computers. This data is derived from the IP addresses of machines connecting back to the command and control server. The majority of infected machines are located in the US, Bangladesh and the UK; however, overall there is wide geographical spread of infections.

Figure 2 shows the country of origin of the organizations targeted by these attacks. While the US and UK again figure highly here, overall the geographical spread is different. This means that the infected computers are rarely located within the organizations' headquarters or country of origin.

Figure 1

Geographic location of infected computers

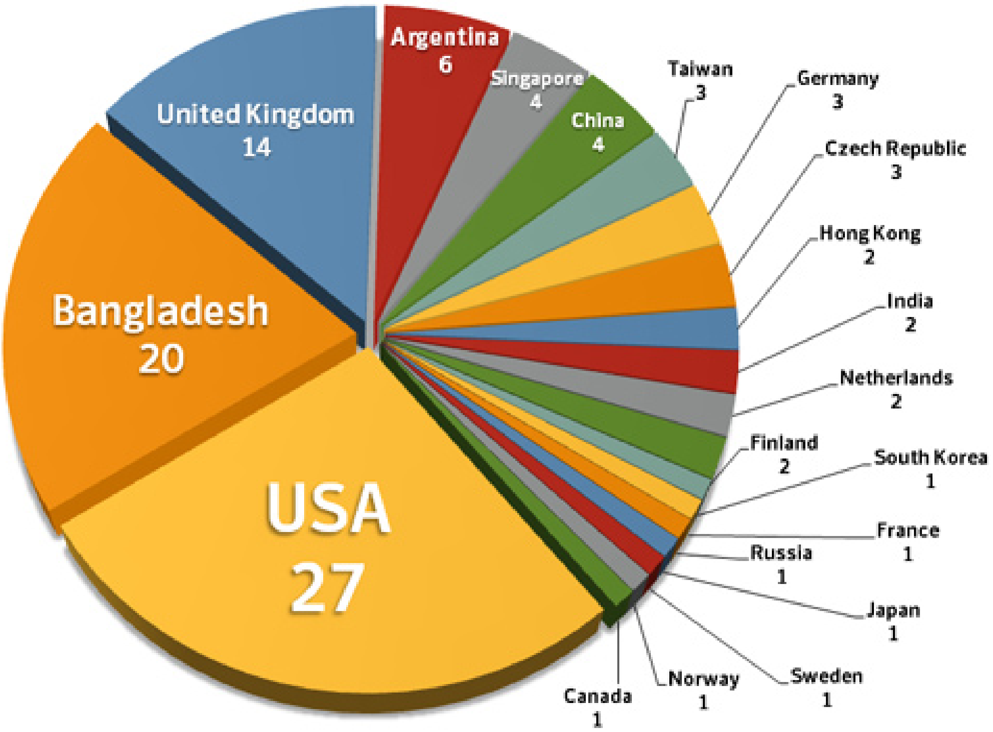
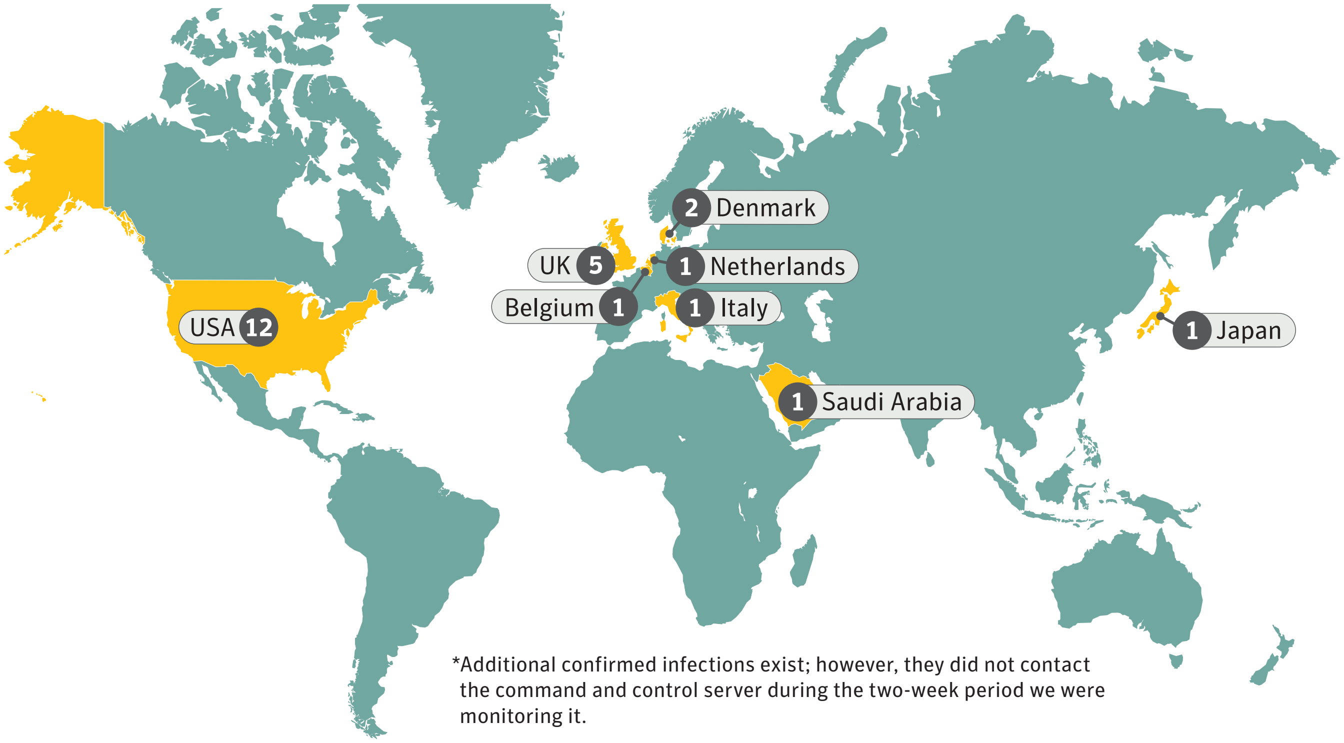


Figure 2

Country of origin of targeted organizations*



*Additional confirmed infections exist; however, they did not contact the command and control server during the two-week period we were monitoring it.

There are two possible explanations for this:

- The attackers are targeting sites, or individuals in certain sites, which they know have access to certain data that is of interest to the attacker.
- The attackers are targeting sites or individuals that they believe have less security measures in place and are therefore an easier access point into the victims' networks.

We can conclude that the attackers are not targeting organizations in a particular country.

Attribution

The attacks were traced back to a computer system that was a virtual private server (VPS) located in the United States. However, the system was owned by a 20-something male located in the Hebei region in China. We internally have given him the pseudonym of Covert Grove based on a literal translation of his name. He attended a vocational school for a short period of time specializing in network security and has limited work experience, most recently maintaining multiple network domains of the vocational school.

Covert Grove claimed to have the U.S.-based VPS for the sole purpose of using the VPS to log into the QQ instant message system, a popular instant messaging system in China. By owning a VPS, he would have a static IP address. He claims this was the sole purpose of the VPS. And by having a static IP address, he could use a feature provided by QQ to restrict login access to particular IP addresses. The VPS cost was RMB200 (US$32) a month. While possible, with an expense of RMB200 a month for such protection and the usage of a US-based VPS, the scenario seems suspicious. We were unable to recover any evidence the VPS was used by any other authorized or unauthorized users. Further, when prompted regarding hacking skills, Covert Grove immediately provided a contact that would perform 'hacking for hire'. Whether this contact is merely an alias or a different individual has not been determined.

We are unable to determine if Covert Grove is the sole attacker or if he has a direct or only indirect role. Nor are we able to definitively determine if he is hacking these targets on behalf of another party or multiple parties.

Technical details

As mentioned above, the threat used to compromise the targeted networks is Poison Ivy, a Remote Access Tool (RAT). This application is freely available from poisonivy-rat.com. It comes fully loaded with a number of plug-ins to give an attacker complete control of the compromised computer.

Delivery

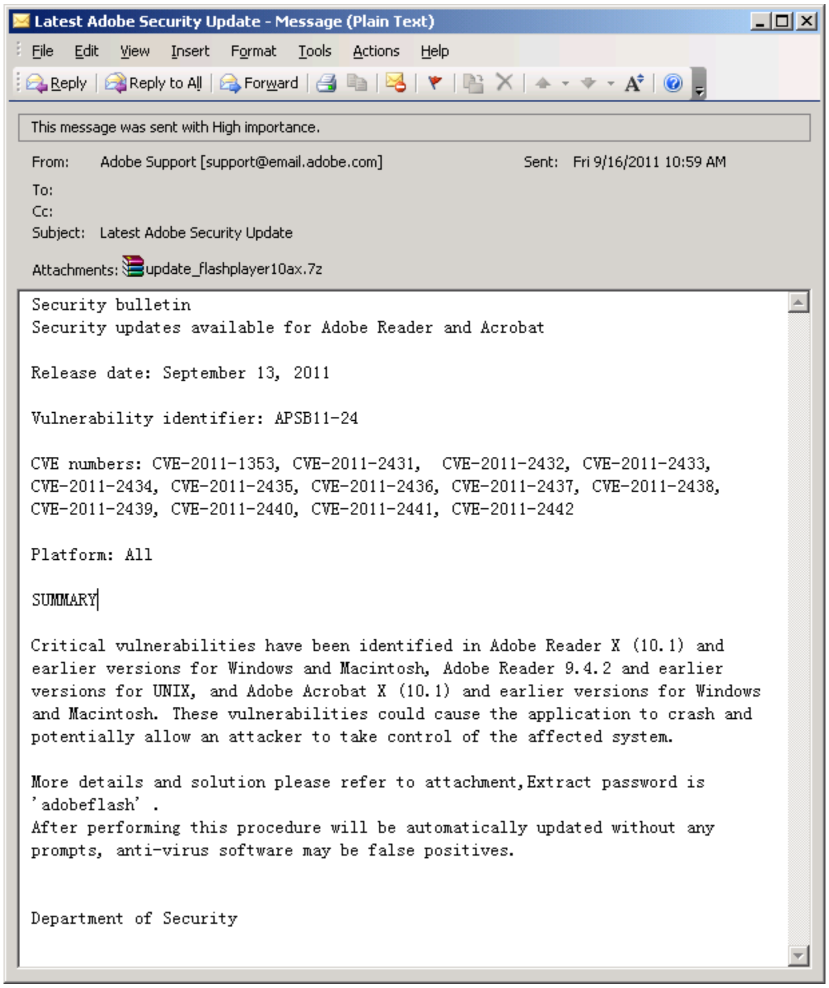
The method of delivery has changed over time as the attackers have changed targets. Older attacks involved a self-extracting archive with a suggestive name, for example: "Human right report of north Africa under the war.scr". The most recent attacks focusing on the chemical industry are using password-protected 7zip files which, when extracted, contain a self-extracting executable. The password to extract the 7zip file is included in the email. This extra stage is used to prevent automated systems from extracting the self-extracting archive. Some example file names using this technique include:

- AntiVirus_update_package.7z
- acquisition.7z
- offer.7z
- update_flashplayer10ax.7z

An example of an email used to send the attachment can be seen in figure 3.

The email is quite generic, applicable to any corporate user. Some of the subject lines will vary and may include the name of the targeted company in an attempt to be more convincing.

Figure 3
Malicious email


Latest Adobe Security Update - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

This message was sent with High importance.

From: Adobe Support [support@email.adobe.com]   Sent: Fri 9/16/2011 10:59 AM
To:
Cc:
Subject: Latest Adobe Security Update

Attachments: update_flashplayer10ax.7z

```
Security bulletin
Security updates available for Adobe Reader and Acrobat

Release date: September 13, 2011

Vulnerability identifier: APSB11-24

CVE numbers: CVE-2011-1353, CVE-2011-2431,  CVE-2011-2432, CVE-2011-2433,
CVE-2011-2434, CVE-2011-2435, CVE-2011-2436, CVE-2011-2437, CVE-2011-2438,
CVE-2011-2439, CVE-2011-2440, CVE-2011-2441, CVE-2011-2442

Platform: All

SUMMARY

Critical vulnerabilities have been identified in Adobe Reader X (10.1) and
earlier versions for Windows and Macintosh, Adobe Reader 9.4.2 and earlier
versions for UNIX, and Adobe Acrobat X (10.1) and earlier versions for Windows
and Macintosh. These vulnerabilities could cause the application to crash and
potentially allow an attacker to take control of the affected system.

More details and solution please refer to attachment,Extract password is
'adobeflash' .
After performing this procedure will be automatically updated without any
prompts, anti-virus software may be false positives.


Department of Security
```

Threat details

When the self-extracting archive file is executed, it will drop two files. Examples of file names that are used include:

- %Temp%\happiness.txt
- %Temp%\xxxx.exe

The executable file, xxxx.exe in this case, is then executed. The second file, happiness.txt, contains custom code in binary format that is encrypted and used by xxxx.exe. The xxxx.exe file copies happiness.txt to C:\PROGRAM FILES\common files\ODBC\ODUBC.DLL and to C:\WINDOWS\system32\jql.sys. It then loads the contents of the encrypted file and injects it into the explorer.exe and iexplore.exe processes.

The injected code copies xxxx.exe to %System%\winsys.exe and connects to the Command and Control (C&C) server on TCP port 80.

The communication with the server is a handshake using an encryption algorithm (Camellia). Once the Trojan establishes the server's authenticity, it expects a variable-size block of binary code that is read from the server straight into the virtual space for iexplore.exe and then executed.

When an executable is compiled, the compiler will store some metadata in the compiled executable. One particular piece of relevant metadata is the location of the compiled code on disk. The path in this instance contained Chinese characters and was:

C:\Documents and Settings\Administrator\桌面\新建文件夹\读取文件\Release\读取文件.pdb

This translates to:

C:\Documents and Settings\Administrator\[Desktop]\[New Folder]\[read the file]\Release\[read the file].pdb

Command and Control (C&C)

When executed, the Poison Ivy threat, or Backdoor.Odivy, connects to a command and control (C&C) server over TCP port 80. A number of different C&C domains and IP addresses were identified. The domains and IPs are listed in table 1.

The majority of samples connect to a domain; however one subset of samples connected directly to the IP address 204.74.215.58, which belonged to the Chinese QQ user mentioned previously and was also associated with antivirus-groups.com.

Table 1

C&C domains and IPs

Domain	IPs
pr[REMOVED].noip.org	173.252.207.71, 173.252.205.36, 173.252.205.37, 173.252.205.64
antivirus-groups.com	74.82.166.205, 204.74.215.58
domain.rm6.org	216.131.95.22, 222.255.28.27
anti-virus.sytes.net	173.252.205.36, 173.252.205.37, 173.252.205.64

Related Attacks

Several other hacker groups have also begun targeting some of the same chemical companies in this time period. Attackers are sending malicious PDF and DOC files, which use exploits to drop variants of Backdoor.Sogu. This particular threat was also used by hackers to compromise a Korean social network site to steal records of 35 million users.

Determining if the two groups are related is difficult, but any relationship appears unlikely. The attackers described in this document use a very basic delivery platform; compressed self-extracting archives sometimes sent to a large number of recipients. The Sogu gang, in contrast, use PDF and DOC files in very tailored, targeted emails. The Sogu gang use a custom developed threat – Backdoor.Sogu, whereas the group described in this document use an off the shelf threat – Poison Ivy. While the number of Sogu targets is currently small relative to the Poison Ivy attacks, we continue to monitor their activities.

Summary

Numerous targeted attack campaigns are occurring every week. However, relative to the total number of attacks, few are fully disclosed. These attacks are primarily targeting private industry in search of key intellectual property for competitive advantage, military institutions, and governmental organizations often in search of documents related to current political events and human rights organizations.

This attack campaign focused on the chemical sector with the goal of obtaining sensitive documents such as proprietary designs, formulas, and manufacturing processes.

Appendix

Example MD5s of PoisonIvy samples used in these attacks:

- 091457444b7e7899c242c5125ddc0571
- 6e99585c3fbd4f3a55bd8f604cb35f38
- 07e266f7fb3c36a1f3a5c5d2d229a478
- 17e7022496d8092d3ca76ae9524a7260
- 2f37912e7cb6e5c478e6dc3d0e381a24
- 5d075e9536c5494745135c1176981c96
- 76000c77ea9a214f5b2ae8cc387809db
- a98d2c90b9494fc885c7cd35d43666ea
- c128c40bd8acb282288e8138352ce4e1
- cab66da82594ff5266ac8dd89e3d1539
- 70fcb3446fce23b18d9a12b2ed911e52
- c53c93a445d751387eb167e5a2b901da
- dd5715cb3b0cdddbe131f03cc08f0f57
- 0f54a9757f1a2fef2b04b776714a7546
- 37f70717f549f1938e5785527e56978d
- 31346e5b39ddb095d76071ac86da4c2e
- 330ddac1f605ff8abf60880c584ed797
- 457a2a8d0784e9fc8e49f6ef60f7f29e
- 87aeec7f7c4ec1b6dc5e6c39b28d8273
- 8d36fd85d9c7d1f4bb170a28cc23498a
- de7e293aa9c4d849dc080f3e87573b24
- 64a4ad90a55e7b6c30c46135435f50a2

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Moutain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

About the authors

Eric Chien is a Technical Director for Security Response and Gavin O’Gorman is a Security Response Manager in Symantec.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call
toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com