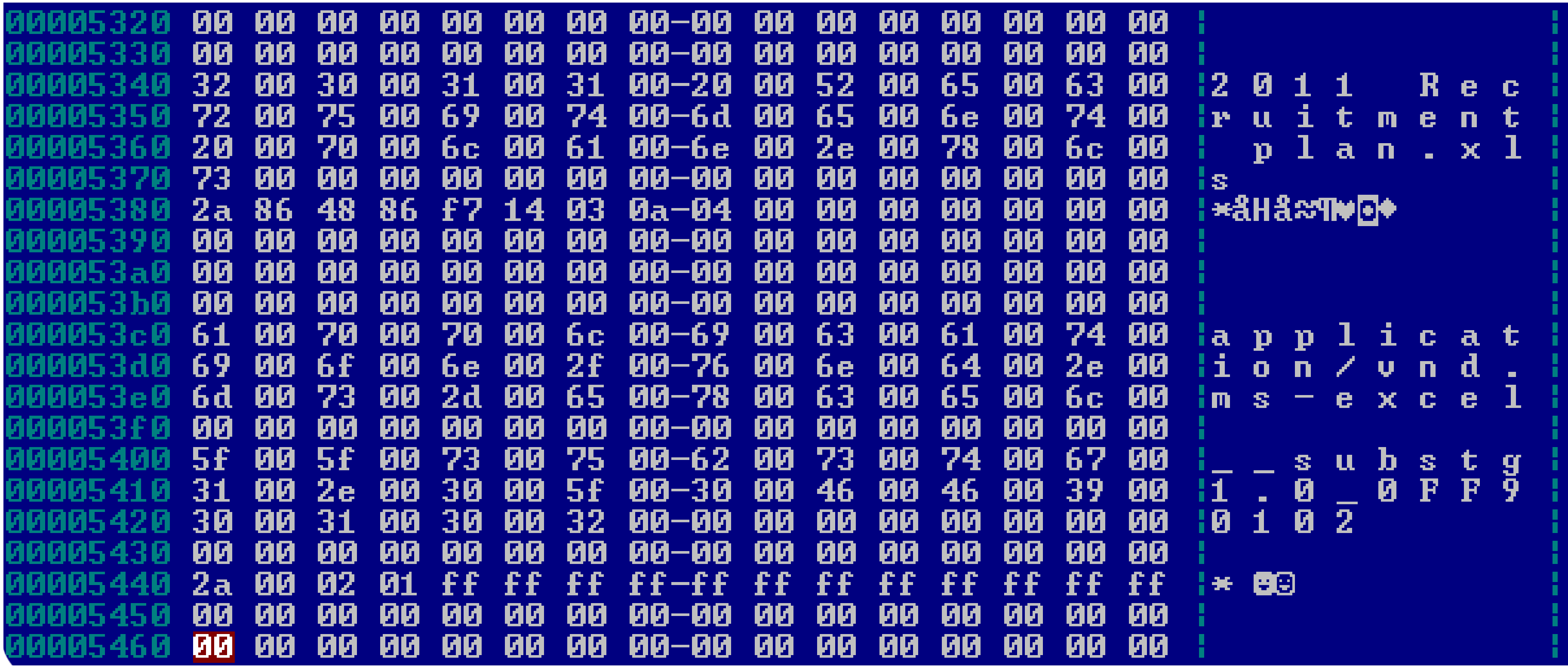


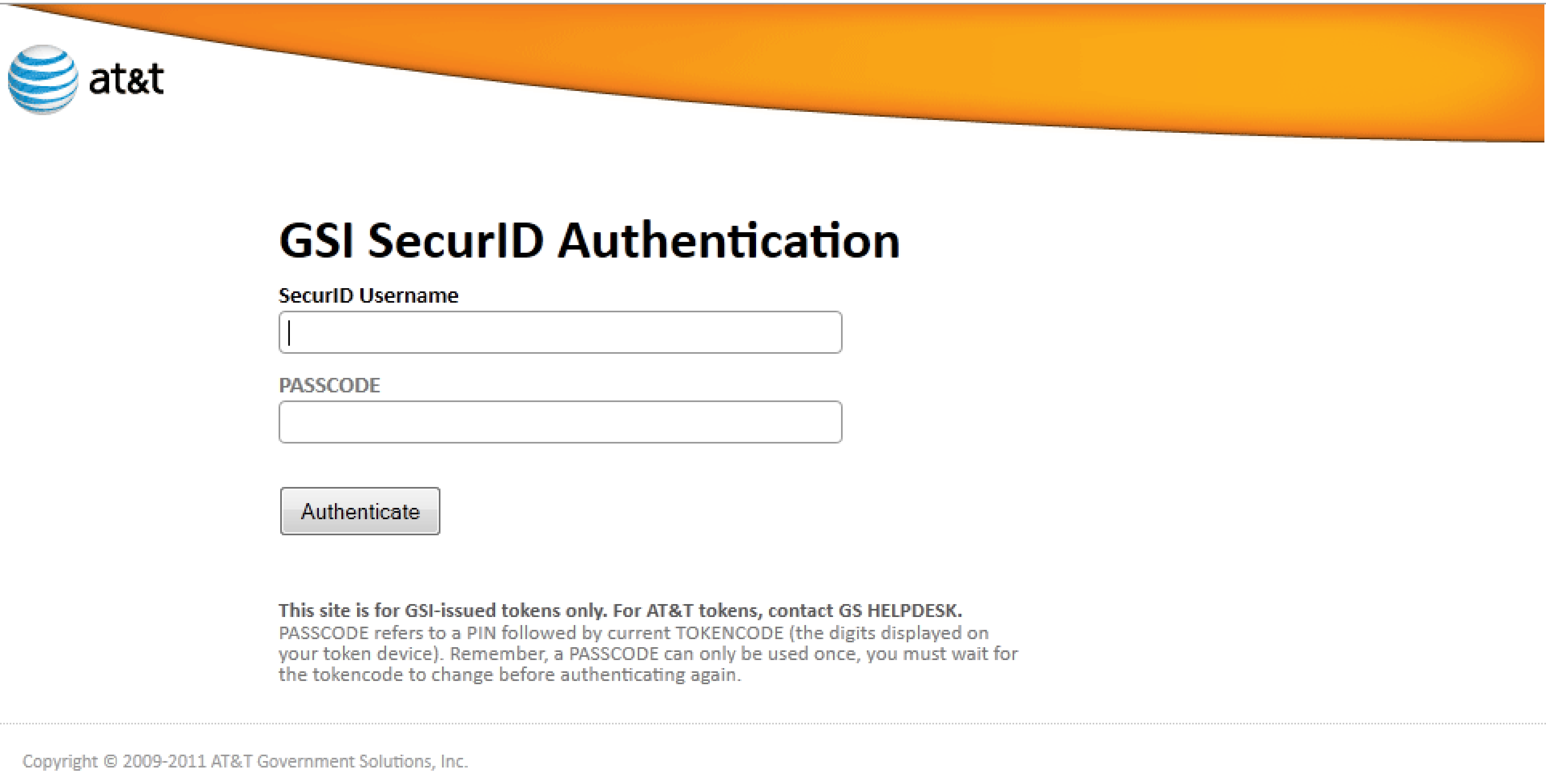
```
00005320 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
00005330 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
00005340 32 00 30 00 31 00 31 00-20 00 52 00 65 00 63 00 ¦2 0 1 1   R e c ¦
00005350 72 00 75 00 69 00 74 00-6d 00 65 00 6e 00 74 00 ¦r u i t m e n t ¦
00005360 20 00 70 00 6c 00 61 00-6e 00 2e 00 78 00 6c 00 ¦  p l a n . x l ¦
00005370 73 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦s               ¦
00005380 2a 86 48 86 f7 14 03 0a-04 00 00 00 00 00 00 00 ¦*åHå≈¶♥◙♦       ¦
00005390 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
000053a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
000053b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
000053c0 61 00 70 00 70 00 6c 00-69 00 63 00 61 00 74 00 ¦a p p l i c a t ¦
000053d0 69 00 6f 00 6e 00 2f 00-76 00 6e 00 64 00 2e 00 ¦i o n / v n d . ¦
000053e0 6d 00 73 00 2d 00 65 00-78 00 63 00 65 00 6c 00 ¦m s - e x c e l ¦
000053f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
00005400 5f 00 5f 00 73 00 75 00-62 00 73 00 74 00 67 00 ¦_ _ s u b s t g ¦
00005410 31 00 2e 00 30 00 5f 00-30 00 46 00 46 00 39 00 ¦1 . 0 _ 0 F F 9 ¦
00005420 30 00 31 00 30 00 32 00-00 00 00 00 00 00 00 00 ¦0 1 0 2         ¦
00005430 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
00005440 2a 00 02 01 ff ff ff ff-ff ff ff ff ff ff ff ff ¦* ☻☺            ¦
00005450 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
00005460 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
```

How RSA Was Breached

Timo Hirvonen 2013-06-18

RSA?

RSA
SecurID®
159 759.
Secured by RSA



GSI SecurID Authentication

SecurID Username

PASSCODE

This site is for GSI-issued tokens only. For AT&T tokens, contact GS HELPDESK.
PASSCODE refers to a PIN followed by current TOKENCODE (the digits displayed on your token device). Remember, a PASSCODE can only be used once, you must wait for the tokencode to change before authenticating again.

The strength of security, broad application support, and variety of authentication methods offered by RSA SecurID authentication have made it the two-factor authentication solution of choice for more than 30,000 organizations and 40 million people worldwide.

RSA brand currently protects more than 250 million online identities

organization is the undisputed market leader with its SecurID family

Attack Timeline

2011-03-14: Adobe Security Advisory

Security bulletin

exploited in the wild

in targeted attacks

via a Flash (.swf) file embedded in Microsoft Excel (.xls) file

CVE-2011-0609

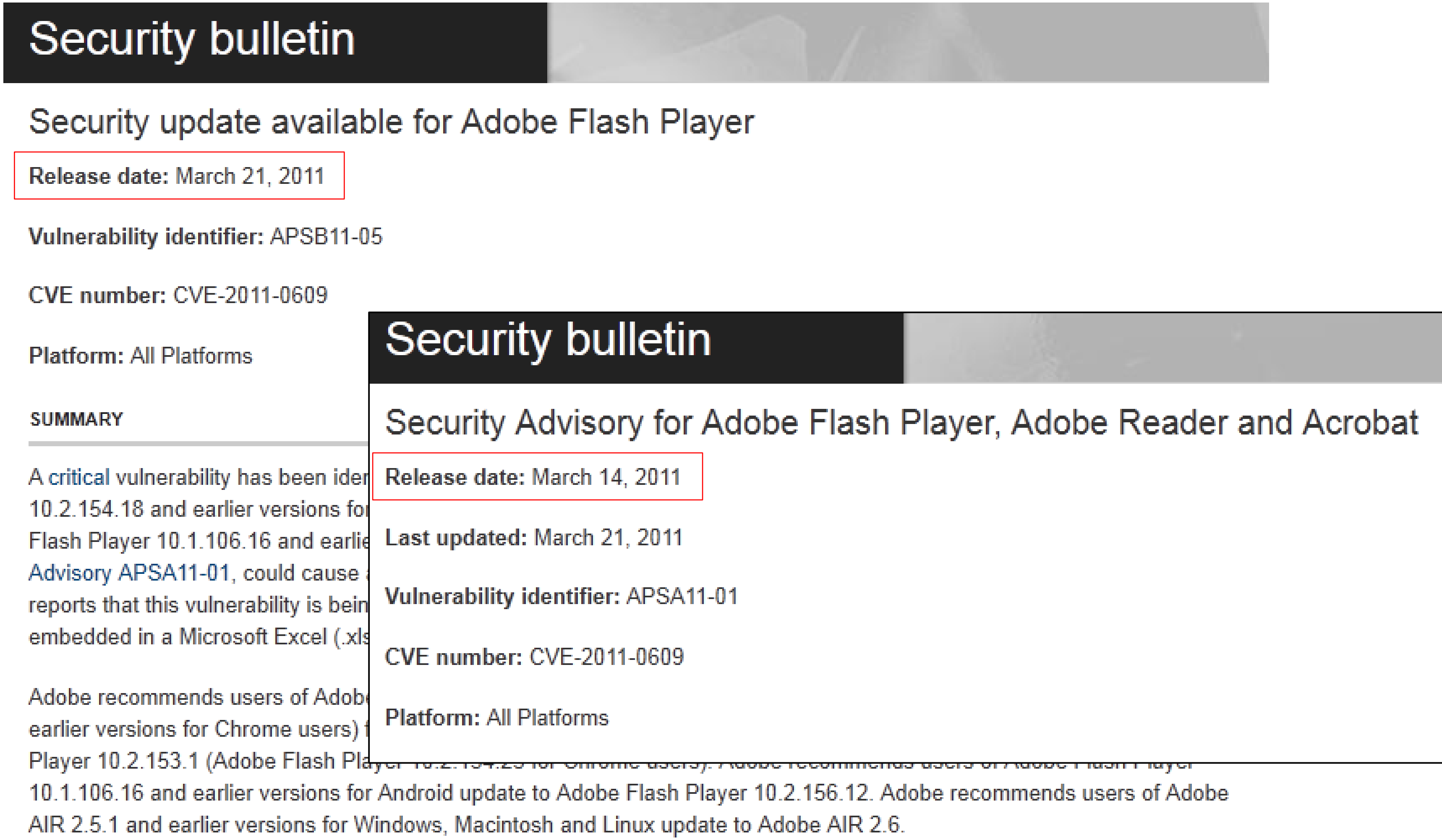
2011-03-17: Open Letter to Customers

Arthur W. Coviello, Jr.

attack resulted in certain information being extracted

information is specifically related to RSA’s SecurID

2011-03-21: Adobe Patch



Security bulletin

Security update available for Adobe Flash Player

Release date: March 21, 2011

Vulnerability identifier: APSB11-05

CVE number: CVE-2011-0609

Platform: All Platforms

SUMMARY

A critical vulnerability has been ider
10.2.154.18 and earlier versions for
Flash Player 10.1.106.16 and earlie
Advisory APSA11-01, could cause
reports that this vulnerability is bein
embedded in a Microsoft Excel (.xls

Adobe recommends users of Adob
earlier versions for Chrome users) t
Player 10.2.153.1 (Adobe Flash Player 10.2.154.25 for Chrome users). Adobe recommends users of Adobe Flash Player 10.1.106.16 and earlier versions for Android update to Adobe Flash Player 10.2.156.12. Adobe recommends users of Adobe AIR 2.5.1 and earlier versions for Windows, Macintosh and Linux update to Adobe AIR 2.6.

Security bulletin

Security Advisory for Adobe Flash Player, Adobe Reader and Acrobat

Release date: March 14, 2011

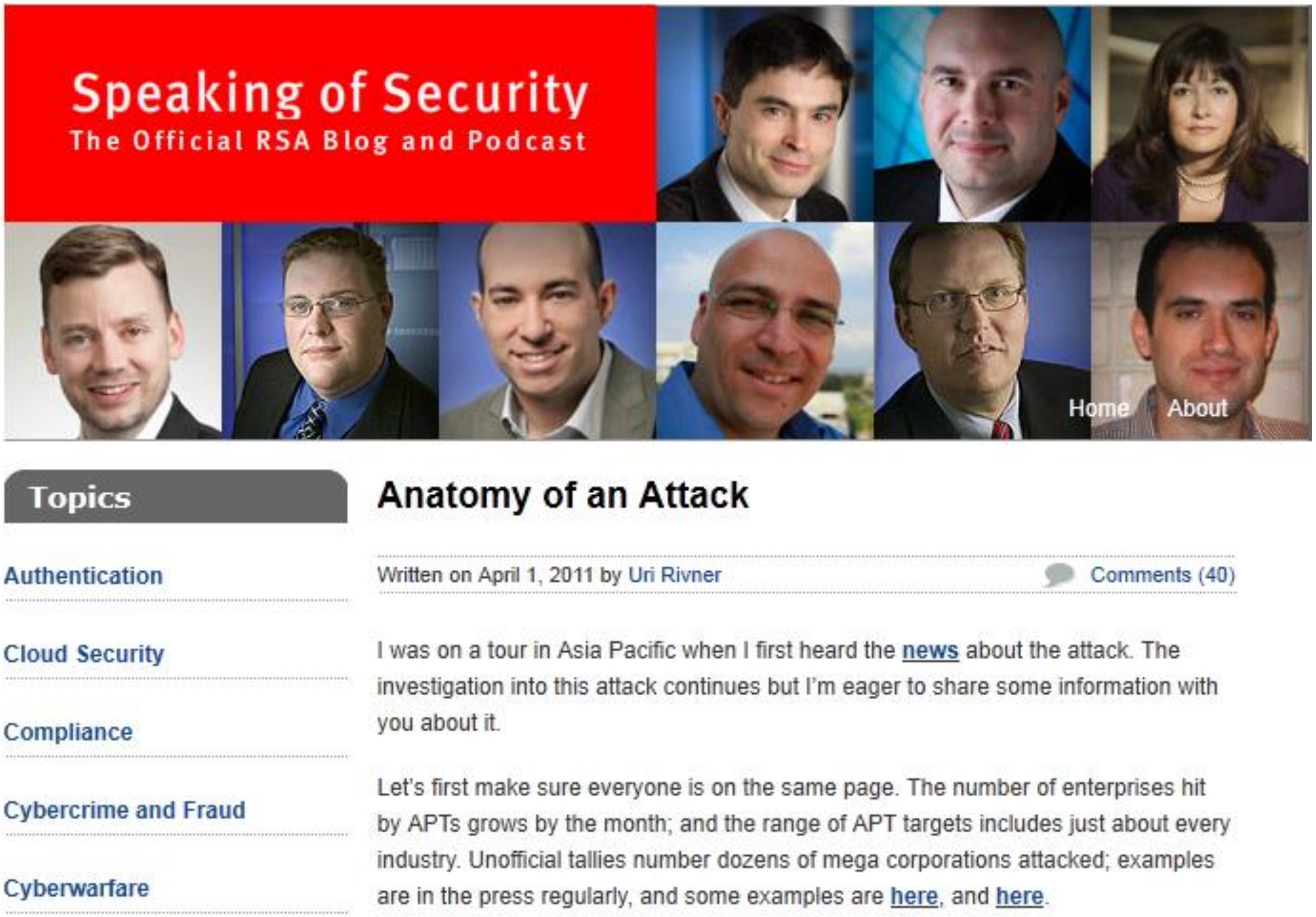
Last updated: March 21, 2011

Vulnerability identifier: APSA11-01

CVE number: CVE-2011-0609

Platform: All Platforms

2011-04-01: RSA blog post Anatomy of an Attack



Anatomy of an Attack

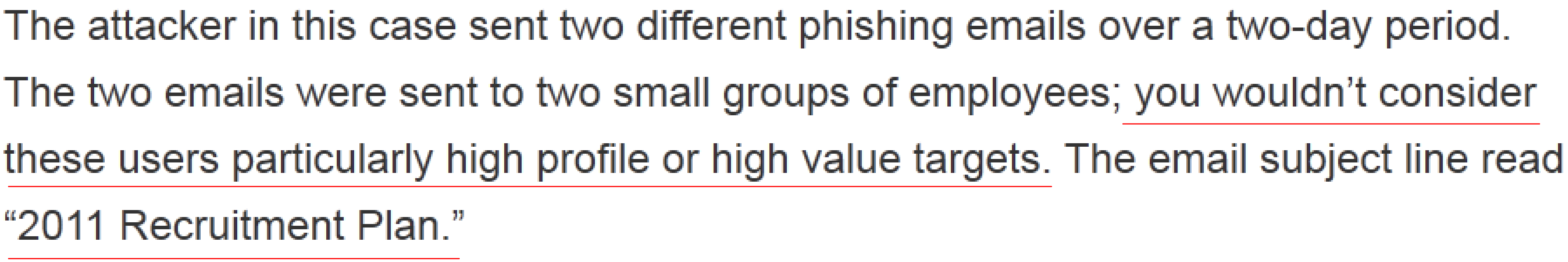
Written on April 1, 2011 by Uri Rivner

Comments (40)

I was on a tour in Asia Pacific when I first heard the news about the attack. The investigation into this attack continues but I'm eager to share some information with you about it.

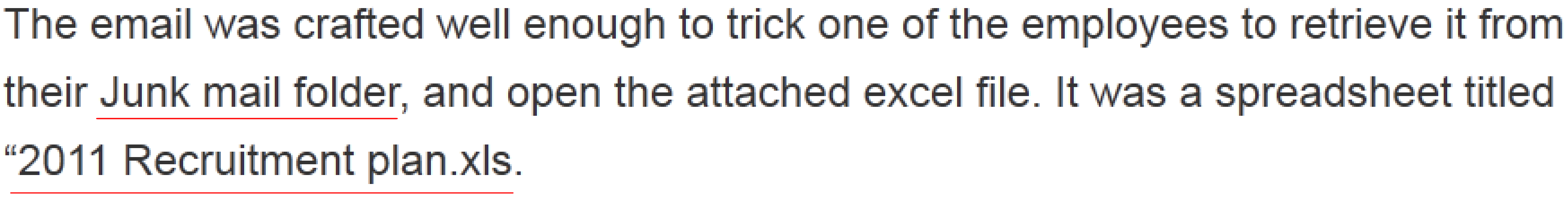
Let's first make sure everyone is on the same page. The number of enterprises hit by APTs grows by the month; and the range of APT targets includes just about every industry. Unofficial tallies number dozens of mega corporations attacked; examples are in the press regularly, and some examples are here, and here.

2011-04-01: RSA blog post Anatomy of an Attack



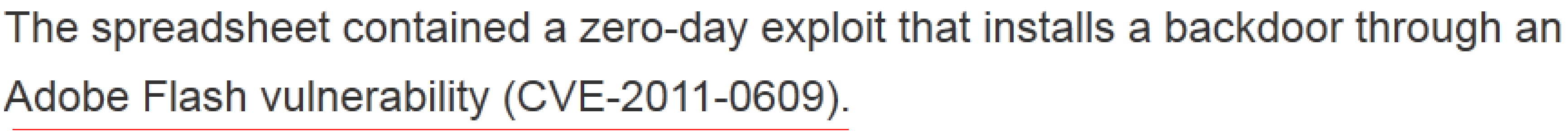
The attacker in this case sent two different phishing emails over a two-day period. The two emails were sent to two small groups of employees; you wouldn't consider these users particularly high profile or high value targets. The email subject line read "2011 Recruitment Plan."

2011-04-01: RSA blog post Anatomy of an Attack



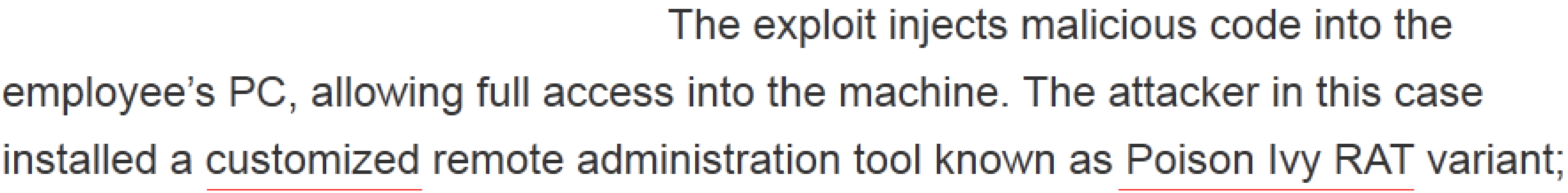
The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached excel file. It was a spreadsheet titled “2011 Recruitment plan.xls.

2011-04-01: RSA blog post Anatomy of an Attack



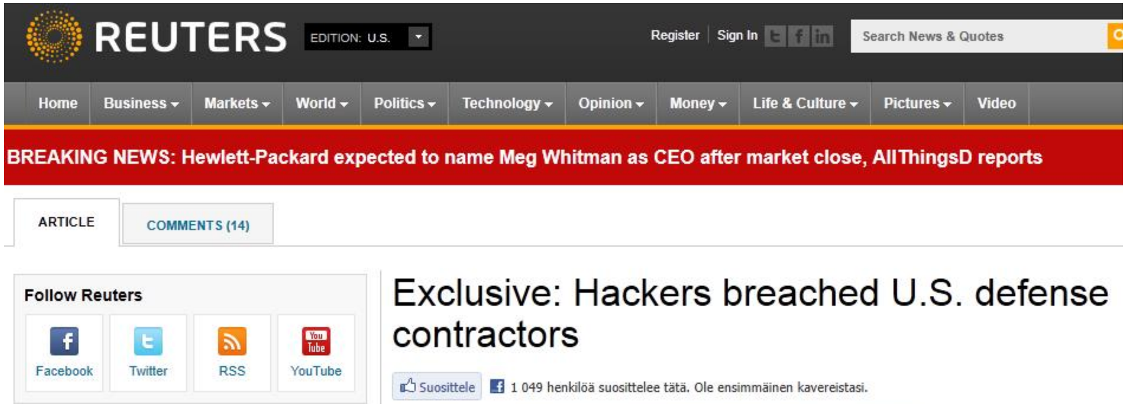
The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability (CVE-2011-0609).

2011-04-01: RSA blog post Anatomy of an Attack



The exploit injects malicious code into the employee's PC, allowing full access into the machine. The attacker in this case installed a customized remote administration tool known as Poison Ivy RAT variant;

2011-05-27: Lockheed Martin Attacked



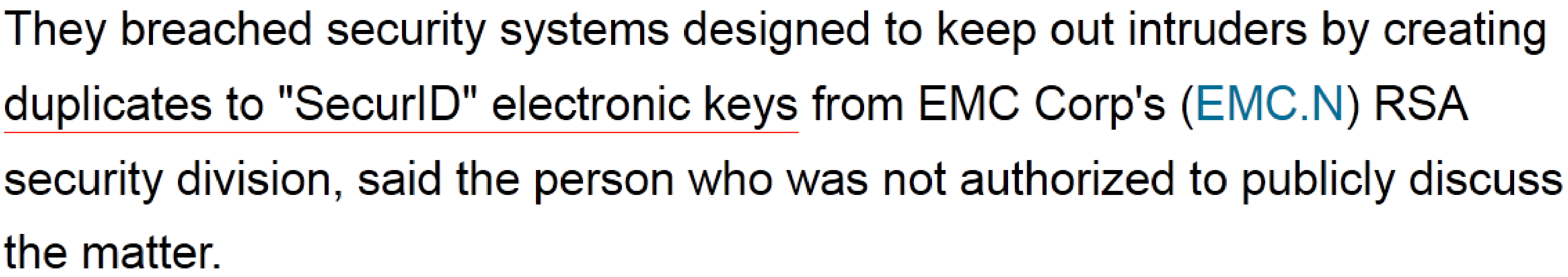
BREAKING NEWS: Hewlett-Packard expected to name Meg Whitman as CEO after market close, AllThingsD reports

Exclusive: Hackers breached U.S. defense contractors

1 049 henkilöä suosittelee tätä. Ole ensimmäinen kavereistasi.

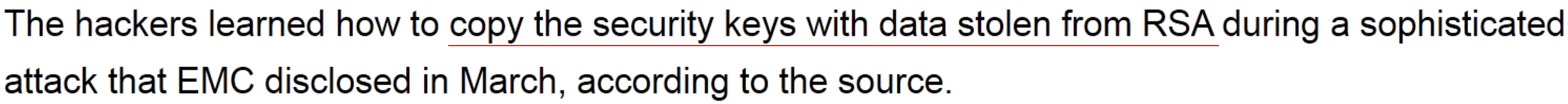
(Reuters) - Unknown hackers have broken into the security networks of Lockheed Martin Corp (LMT.N) and several other U.S. military contractors, a source with direct knowledge of the attacks told Reuters.

2011-05-27: Lockheed Martin Attacked



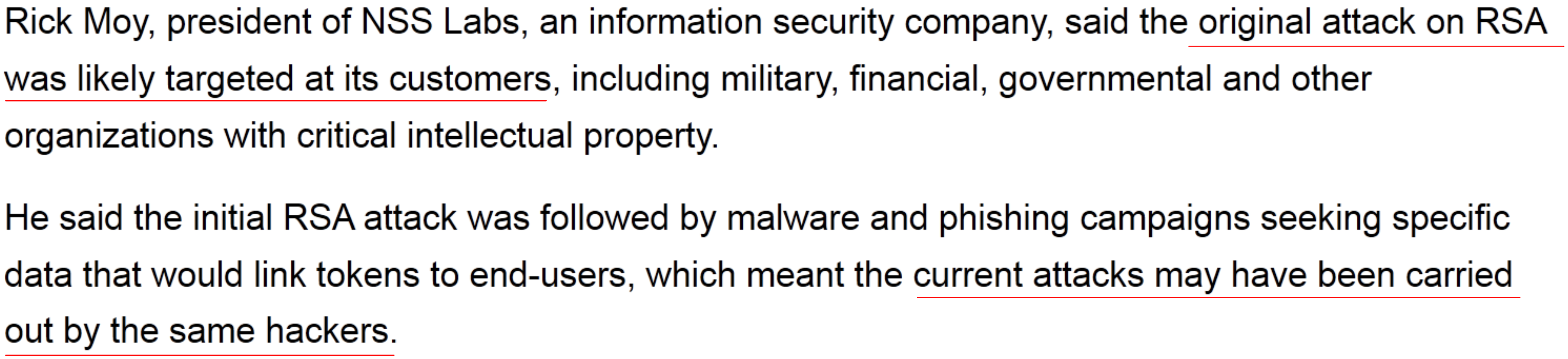
They breached security systems designed to keep out intruders by creating duplicates to "SecurID" electronic keys from EMC Corp's (EMC.N) RSA security division, said the person who was not authorized to publicly discuss the matter.

2011-05-27: Lockheed Martin Attacked



The hackers learned how to copy the security keys with data stolen from RSA during a sophisticated attack that EMC disclosed in March, according to the source.

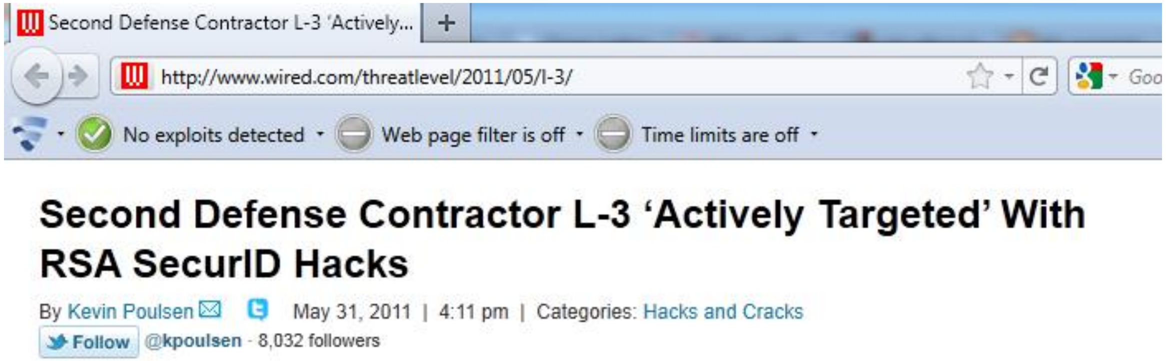
2011-05-27: Lockheed Martin Attacked



Rick Moy, president of NSS Labs, an information security company, said the original attack on RSA was likely targeted at its customers, including military, financial, governmental and other organizations with critical intellectual property.

He said the initial RSA attack was followed by malware and phishing campaigns seeking specific data that would link tokens to end-users, which meant the current attacks may have been carried out by the same hackers.

2011-05-31: L-3 Communications targeted



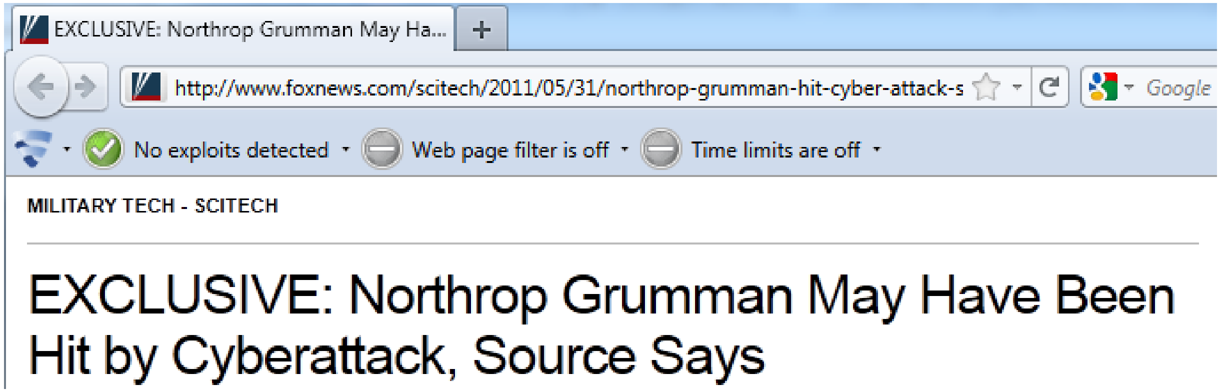
Second Defense Contractor L-3 'Actively...
http://www.wired.com/threatlevel/2011/05/l-3/
Goo
No exploits detected
Web page filter is off
Time limits are off

Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks

By Kevin Poulsen May 31, 2011 | 4:11 pm | Categories: Hacks and Cracks
Follow @kpoulsen · 8,032 followers

"L-3 Communications has been actively targeted with penetration attacks leveraging the compromised information," read an April 6 e-mail from an executive at L-3's Stratus Group to the group's 5,000 workers, one of whom shared the contents with Wired.com on condition of anonymity.

2011-06-01: Northrop Grumman



EXCLUSIVE: Northrop Grumman May Ha...

http://www.foxnews.com/scitech/2011/05/31/northrop-grumman-hit-cyber-attack-s

No exploits detected

Web page filter is off

Time limits are off

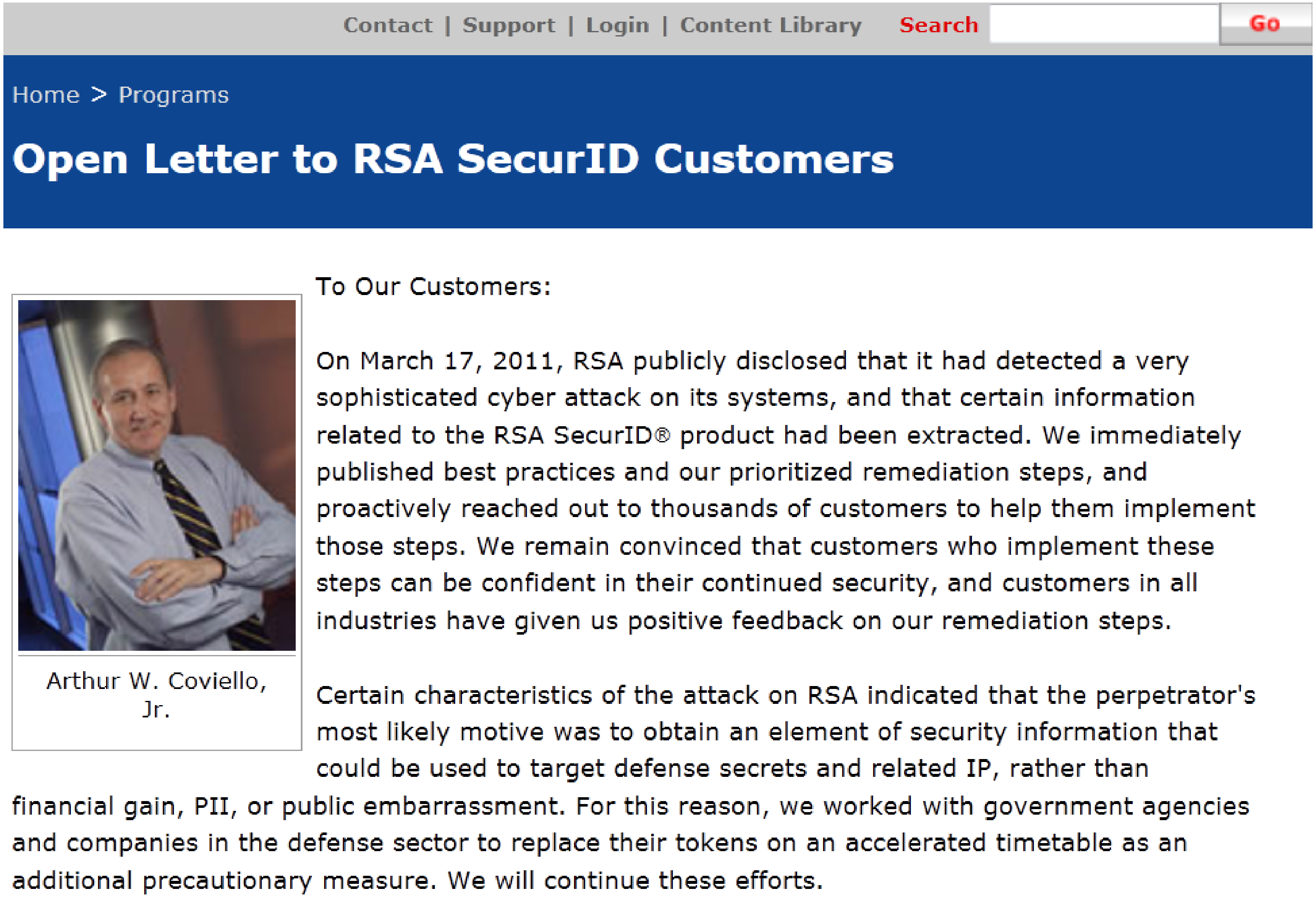
MILITARY TECH - SCITECH

EXCLUSIVE: Northrop Grumman May Have Been Hit by Cyberattack, Source Says

On May 26, Northrop Grumman shut down remote access to its network without warning -- catching even senior managers by surprise and leading to speculation that a similar breach had occurred.

"We do not comment on whether or not Northrop Grumman is or has been a target for cyber intrusions,"

2011-06-06: RSA Admits SecurID Compromise



Open Letter to RSA SecurID Customers

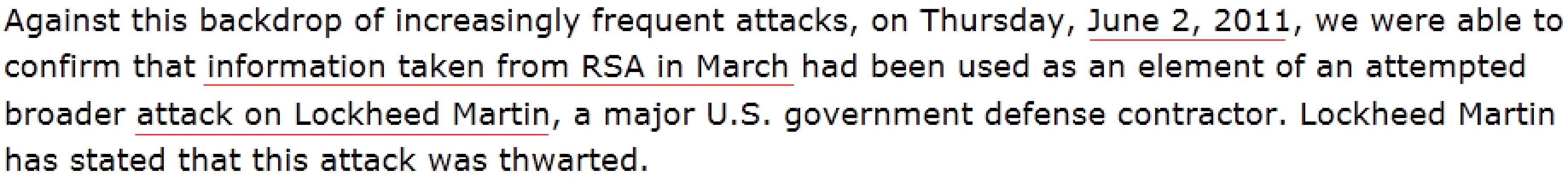
Arthur W. Coviello, Jr.

To Our Customers:

On March 17, 2011, RSA publicly disclosed that it had detected a very sophisticated cyber attack on its systems, and that certain information related to the RSA SecurID® product had been extracted. We immediately published best practices and our prioritized remediation steps, and proactively reached out to thousands of customers to help them implement those steps. We remain convinced that customers who implement these steps can be confident in their continued security, and customers in all industries have given us positive feedback on our remediation steps.

Certain characteristics of the attack on RSA indicated that the perpetrator's most likely motive was to obtain an element of security information that could be used to target defense secrets and related IP, rather than financial gain, PII, or public embarrassment. For this reason, we worked with government agencies and companies in the defense sector to replace their tokens on an accelerated timetable as an additional precautionary measure. We will continue these efforts.

2011-06-06: RSA Admits SecurID Compromise

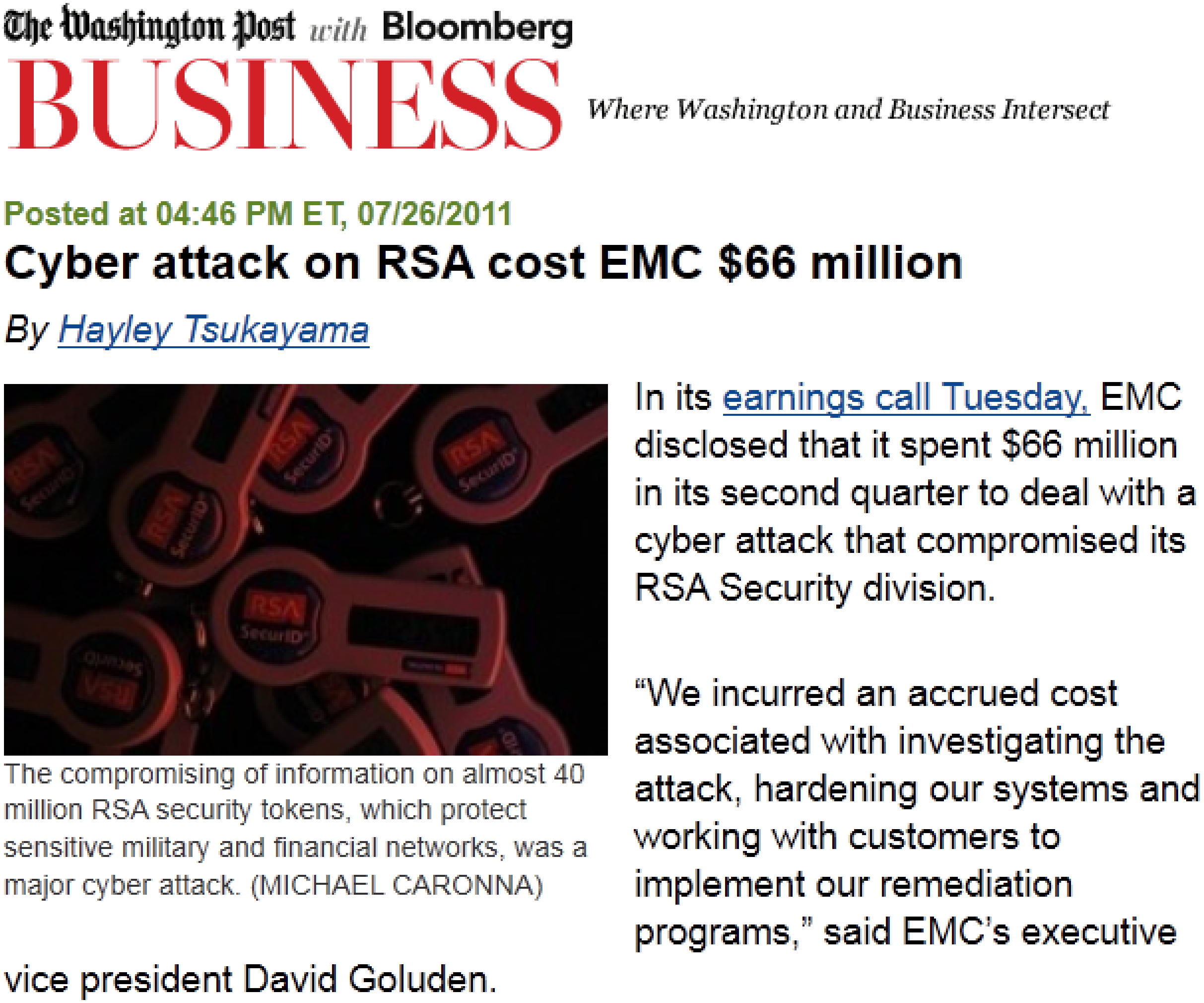


Against this backdrop of increasingly frequent attacks, on Thursday, June 2, 2011, we were able to confirm that information taken from RSA in March had been used as an element of an attempted broader attack on Lockheed Martin, a major U.S. government defense contractor. Lockheed Martin has stated that this attack was thwarted.

2011-06-06: RSA Admits SecurID Compromise

An offer to replace SecurID tokens for customers with concentrated user bases typically focused on protecting intellectual property and corporate networks.

2011-07-26: Cost of RSA Breach: $66 Million



The Washington Post *with* Bloomberg

BUSINESS *Where Washington and Business Intersect*

Posted at 04:46 PM ET, 07/26/2011

Cyber attack on RSA cost EMC $66 million

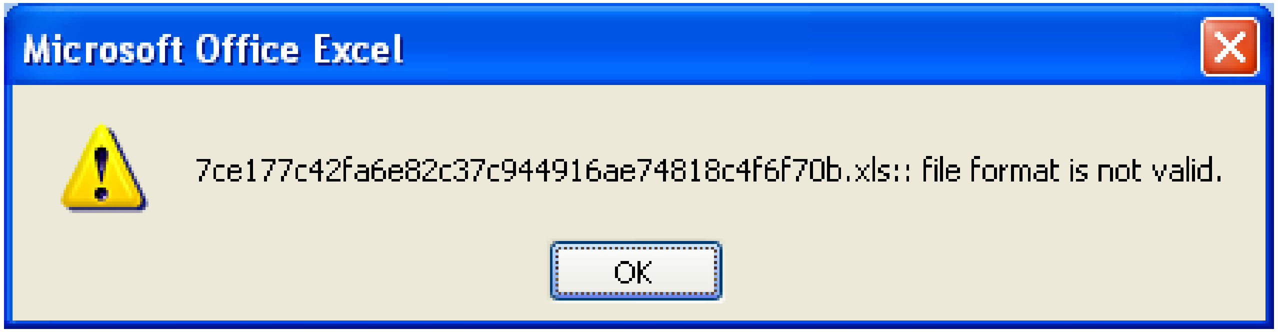
By Hayley Tsukayama

The compromising of information on almost 40 million RSA security tokens, which protect sensitive military and financial networks, was a major cyber attack. (MICHAEL CARONNA)

In its earnings call Tuesday, EMC disclosed that it spent $66 million in its second quarter to deal with a cyber attack that compromised its RSA Security division.

"We incurred an accrued cost associated with investigating the attack, hardening our systems and working with customers to implement our remediation programs," said EMC's executive vice president David Goluden.

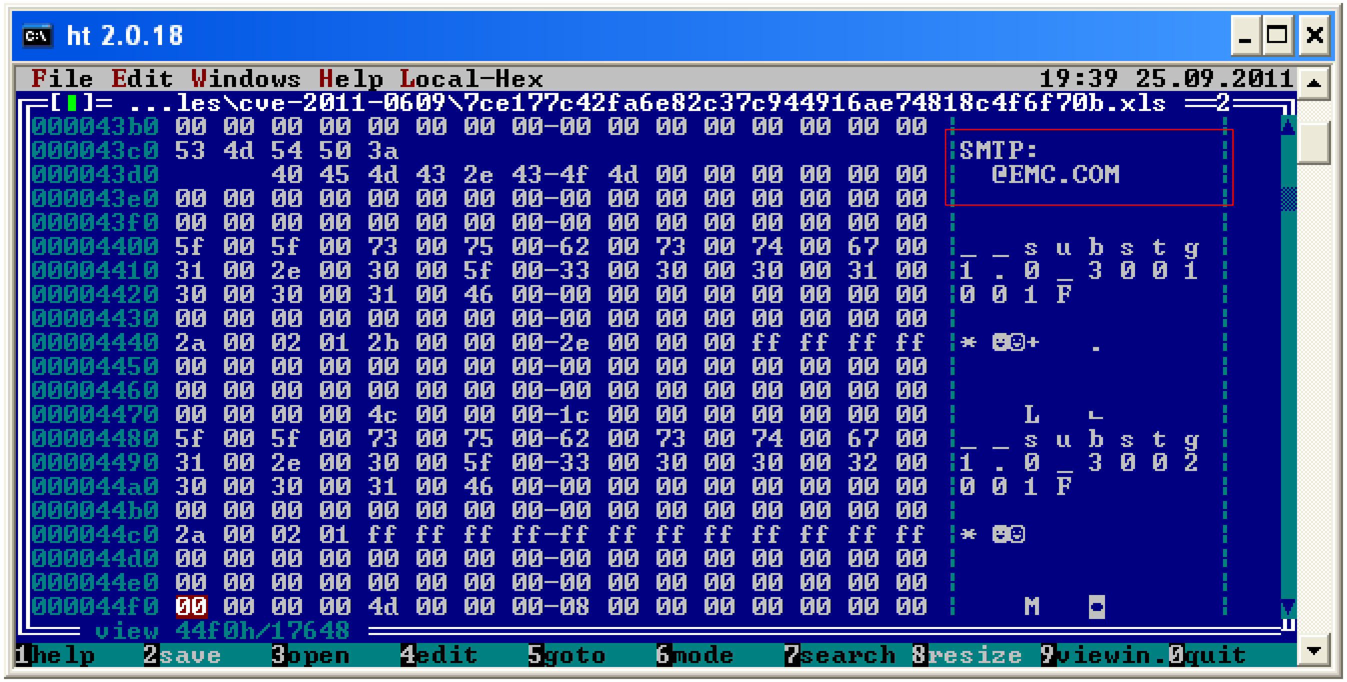
2011-08-22: Email Discovered



Microsoft Office Excel

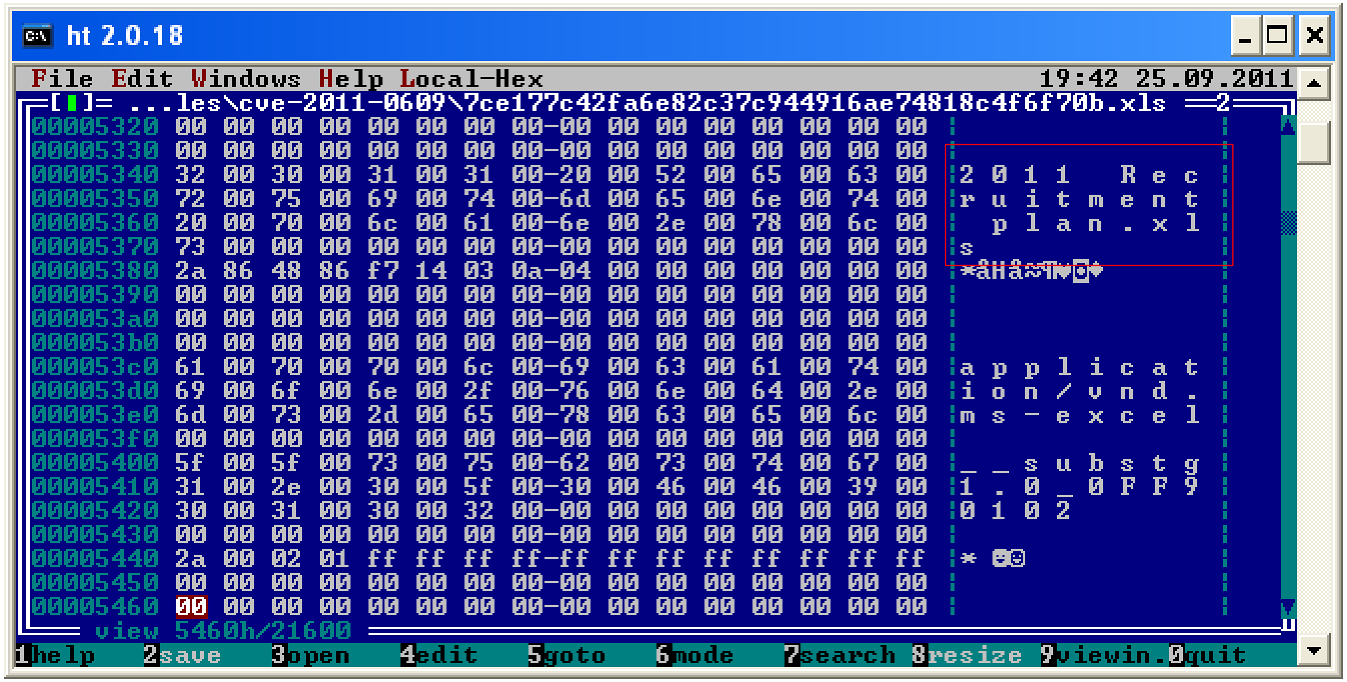
7ce177c42fa6e82c37c944916ae74818c4f6f70b.xls:: file format is not valid.

2011-08-22: Email Discovered



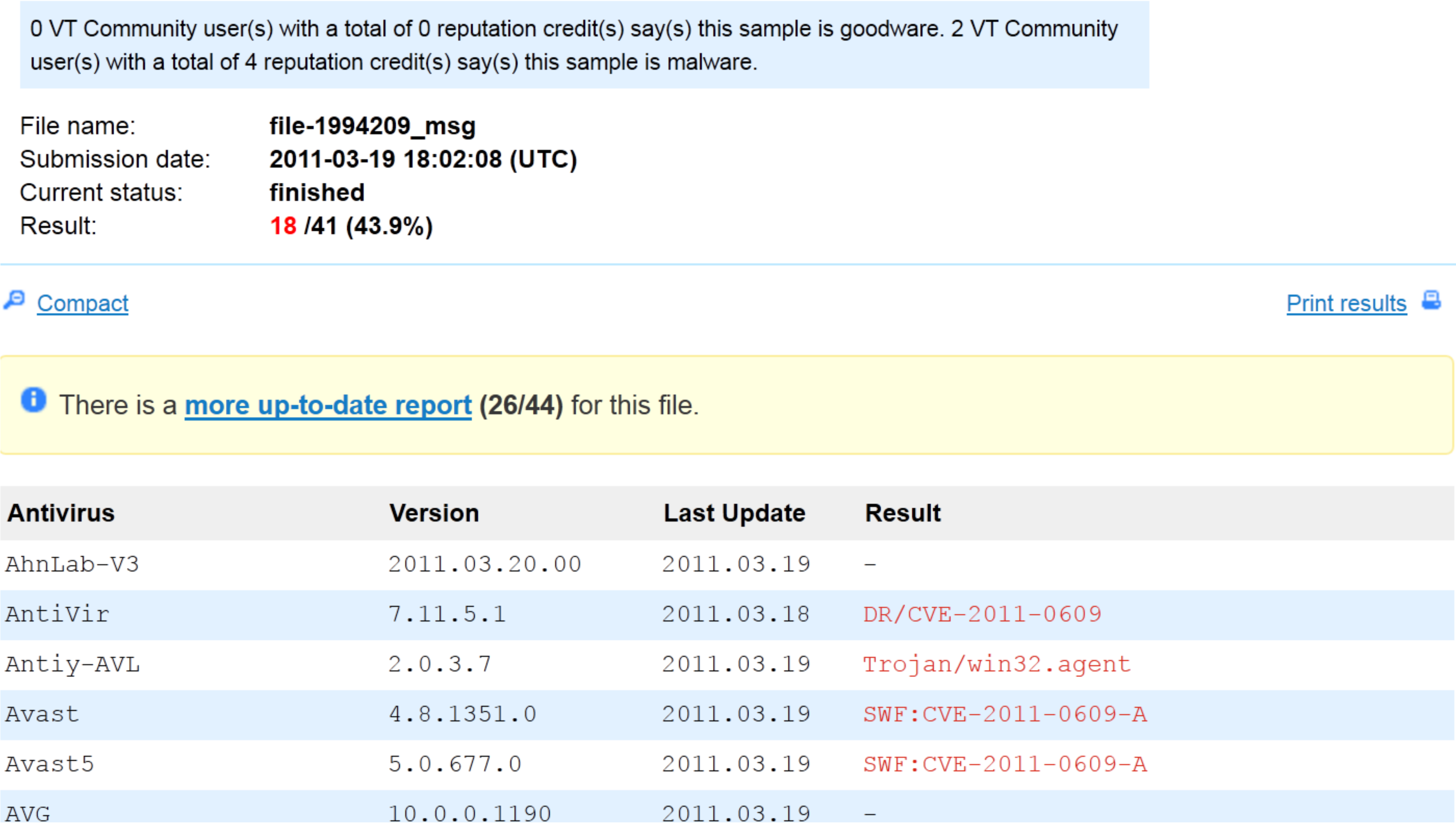
```
File Edit Windows Help Local-Hex                                    19:39 25.09.2011
[■]= ...les\cve-2011-0609\7ce177c42fa6e82c37c944916ae74818c4f6f70b.xls =2=
000043b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
000043c0 53 4d 54 50 3a                                  ¦SMTP:           ¦
000043d0                40 45 4d 43 2e 43-4f 4d 00 00 00 00 00 00 ¦   @EMC.COM      ¦
000043e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
000043f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
00004400 5f 00 5f 00 73 00 75 00-62 00 73 00 74 00 67 00 ¦_ _ s u b s t g ¦
00004410 31 00 2e 00 30 00 5f 00-33 00 30 00 30 00 31 00 ¦1 . 0 _ 3 0 0 1 ¦
00004420 30 00 30 00 31 00 46 00-00 00 00 00 00 00 00 00 ¦0 0 1 F         ¦
00004430 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
00004440 2a 00 02 01 2b 00 00 00-2e 00 00 00 ff ff ff ff ¦* ☻☺+   .       ¦
00004450 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
00004460 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
00004470 00 00 00 00 4c 00 00 00-1c 00 00 00 00 00 00 00 ¦    L   ∟       ¦
00004480 5f 00 5f 00 73 00 75 00-62 00 73 00 74 00 67 00 ¦_ _ s u b s t g ¦
00004490 31 00 2e 00 30 00 5f 00-33 00 30 00 30 00 32 00 ¦1 . 0 _ 3 0 0 2 ¦
000044a0 30 00 30 00 31 00 46 00-00 00 00 00 00 00 00 00 ¦0 0 1 F         ¦
000044b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
000044c0 2a 00 02 01 ff ff ff ff-ff ff ff ff ff ff ff ff ¦* ☻☺            ¦
000044d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
000044e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ¦                ¦
000044f0 00 00 00 00 4d 00 00 00-08 00 00 00 00 00 00 00 ¦    M   ◘       ¦
 view 44f0h/17648
1help 2save 3open 4edit 5goto 6mode 7search 8resize 9viewin.0quit
```

2011-08-22: Email Discovered



```
ht 2.0.18
 File  Edit  Windows  Help  Local-Hex                                19:42  25.09.2011
[ ]= ...les\cve-2011-0609\7ce177c42fa6e82c37c944916ae74818c4f6f70b.xls ═2═
00005320 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00005330 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00005340 32 00 30 00 31 00 31 00-20 00 52 00 65 00 63 00 2 0 1 1   R e c
00005350 72 00 75 00 69 00 74 00-6d 00 65 00 6e 00 74 00 r u i t m e n t
00005360 20 00 70 00 6c 00 61 00-6e 00 2e 00 78 00 6c 00   p l a n . x l
00005370 73 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 s
00005380 2a 86 48 86 f7 14 03 0a-04 00 00 00 00 00 00 00 *åHå≈¶♥◙♦
00005390 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
000053a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
000053b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
000053c0 61 00 70 00 70 00 6c 00-69 00 63 00 61 00 74 00 a p p l i c a t
000053d0 69 00 6f 00 6e 00 2f 00-76 00 6e 00 64 00 2e 00 i o n / v n d .
000053e0 6d 00 73 00 2d 00 65 00-78 00 63 00 65 00 6c 00 m s - e x c e l
000053f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00005400 5f 00 5f 00 73 00 75 00-62 00 73 00 74 00 67 00 _ _ s u b s t g
00005410 31 00 2e 00 30 00 5f 00-30 00 46 00 46 00 39 00 1 . 0 _ 0 F F 9
00005420 30 00 31 00 30 00 32 00-00 00 00 00 00 00 00 00 0 1 0 2
00005430 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00005440 2a 00 02 01 ff ff ff ff-ff ff ff ff ff ff ff ff *  ☻☺
00005450 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00005460 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
    view 5460h/21600
1help  2save  3open  4edit  5goto  6mode  7search 8resize 9viewin.0quit
```

2011-03-19: Email Uploaded to VirusTotal



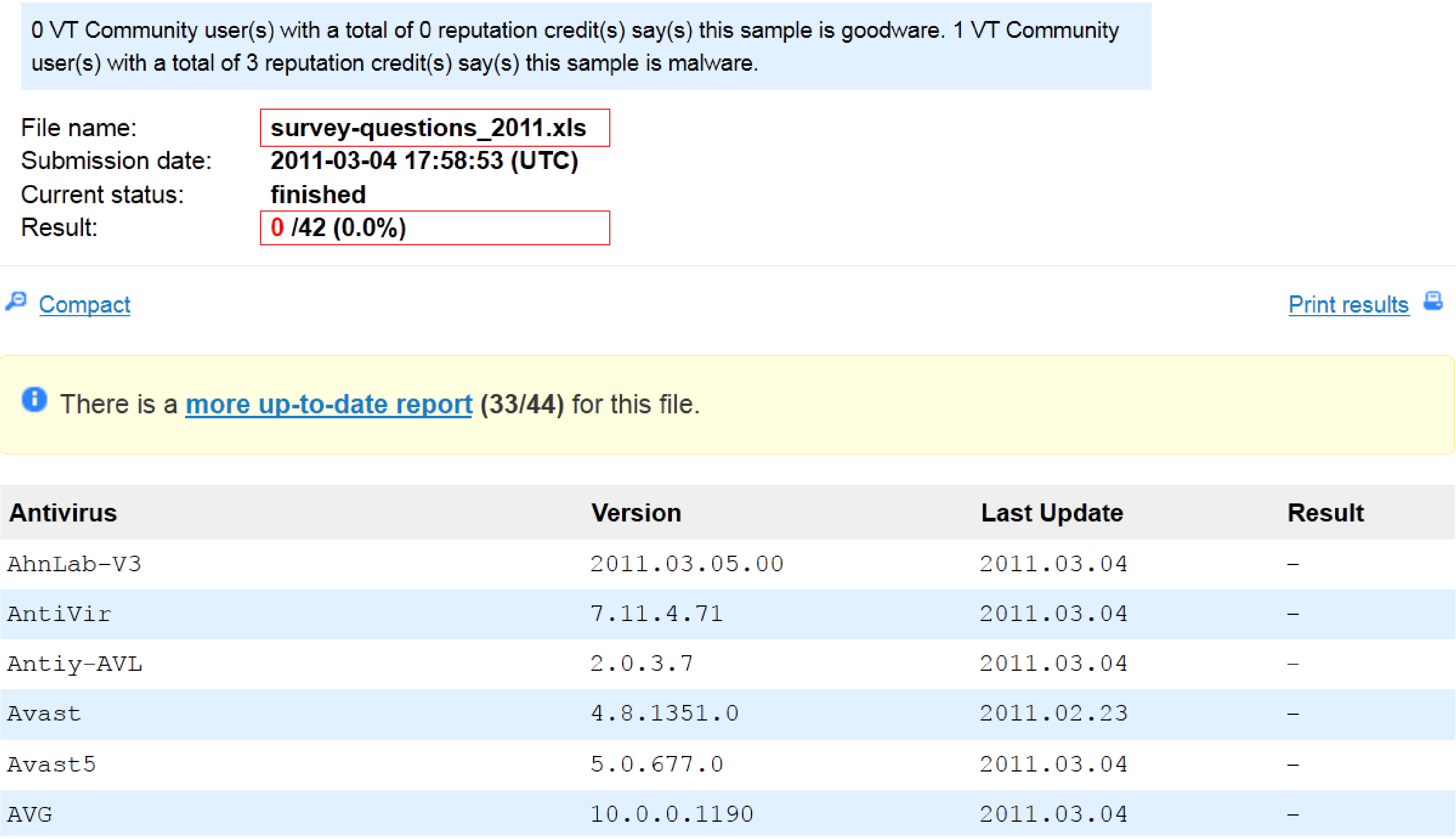
0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 2 VT Community user(s) with a total of 4 reputation credit(s) say(s) this sample is malware.

File name:	**file-1994209_msg**
Submission date:	**2011-03-19 18:02:08 (UTC)**
Current status:	**finished**
Result:	**18 /41 (43.9%)**

ℹ There is a more up-to-date report **(26/44)** for this file.

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.03.20.00	2011.03.19	-
AntiVir	7.11.5.1	2011.03.18	DR/CVE-2011-0609
Antiy-AVL	2.0.3.7	2011.03.19	Trojan/win32.agent
Avast	4.8.1351.0	2011.03.19	SWF:CVE-2011-0609-A
Avast5	5.0.677.0	2011.03.19	SWF:CVE-2011-0609-A
AVG	10.0.0.1190	2011.03.19	-

2011-03-04: Excel file uploaded to VirusTotal



0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 1 VT Community user(s) with a total of 3 reputation credit(s) say(s) this sample is malware.

File name:	**survey-questions_2011.xls**
Submission date:	**2011-03-04 17:58:53 (UTC)**
Current status:	**finished**
Result:	**0 /42 (0.0%)**

There is a more up-to-date report **(33/44)** for this file.

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.03.05.00	2011.03.04	–
AntiVir	7.11.4.71	2011.03.04	–
Antiy-AVL	2.0.3.7	2011.03.04	–
Avast	4.8.1351.0	2011.02.23	–
Avast5	5.0.677.0	2011.03.04	–
AVG	10.0.0.1190	2011.03.04	–

Demo Time

What Would Have Stopped the Infection?

What Would Have Stopped the Infection?

- Uninstalling Flash, or disabling Flash content in Microsoft Office

- Limited user account

- Office 2010

- Windows 7

- Microsoft EMET

Thank You!

timo.hirvonen@f-secure.com

Protecting
the
irreplaceable

F-Secure.