The “MSUpdater” Trojan
And Ongoing Targeted Attacks

A Zscaler and Seculert Joint Report

Contents

Overview

Researchers from Zscaler and Seculert separately identified incidents and threats discussed in this report. Within a private security forum we discussed and determined that we had identified related incidents. Zscaler and Seculert collaborated on this report to aggregate and correlate our findings along with open-source intelligence (OSINT) to detail a lesser-known “MSUpdater” remote access Trojan (RAT) and its linkage to current targeted attacks and others dating back to at least early 2009. Foreign and domestic (United States) companies with intellectual property dealing in aero/geospace and defense seem to be some of the recent industries targeted in these attacks.

The goal of this report is to aggregate information, draw some correlations, and provide an overview of this threat to facilitate its identification, detection, and functionality. With this goal in mind, we also aim not to reveal anything that might disrupt any investigations or state something without additional open-source corroboration. We as security researchers believe that our success is not measured by how much information we collect, but in how we use and share the information to better secure and protect the Internet community from threats. We hope that the information within this report helps to detect and remediate this threat within organizations.

“MSUpdater” Trojan Incidents Observed

Zscaler and Seculert separately identified security incidents where infected customers in the fore-mentioned industries had command and control (C&C) beacons matching the below patterns. Standard Microsoft Internet Explorer user-agent strings (versions 6 – 8) were observed for the C&C communications.

The most often observed pattern, and likely the C&C “check-in” behavior followed the pattern:

- HTTP GET requests to the path: /microsoftupdate/getupdate/default.aspx?ID=[num1]para1=[num2]para2=[num3]para3=[num4]

Where the [num] fields are placeholders for parameters passed by the victim in the form of numbers.

Other patterns observed from the infected hosts to the C&Cs were:

- HTTP GET and POST requests to the path: /microsoft/errorpost/default/connect.aspx?ID=[num1]
- HTTP POSTs to the path: /microsoft/errorpost/default.aspx?ID=[num1]

Clearly the above patterns are trying to appear as though they are related to Microsoft’s “Windows Update” service versus something malicious. A clear, common name for this particular threat did not seem to emerge in the open-source, so we have commonly referred to this threat family as the “MSUpdater” Trojan.

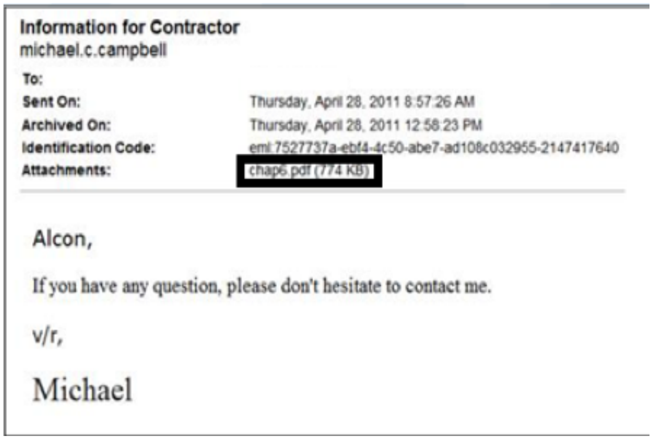
The first time this pattern was logged in traffic traversing Zscaler’s Cloud infrastructure was on 12/25/2010 (Christmas day). It is likely that the Christmas day infection resulted from a targeted phishing email as related attacks in this report identify this as the infection vector. No suspicious web transactions were observed from the infected host prior to the C&C beaconing. Seculert FogSense Cloud-based service observed instances of this same infected beaconing pattern for their customers as early as March 2010. Zscaler and Seculert each identified these infections separately by conducting traffic analysis to identify previously unknown threats to then protect their customers. Open-source intelligence (OSINT) on the beaconing patterns we observed provided additional information to this previous threat.

OSINT Aggregation and Correlation

In addition to industry collaboration to better understand and protect against threats, “Google” or more specifically OSINT is a valuable resource when looking into “unidentified” threats. The following provides some details about what is known and has been discussed in the open-source related to this threat.

Infection Vector: Phishing Email with Malicious Attachment

A publicly available presentation from *Sword & Shield Enterprise Security Inc.*[1] includes a slide discussing the correlation of a malicious phishing attachment to C&C beaconing that resembles the same pattern identified above. Specifically, the presentation provides a screenshot of an associated malicious phishing email showing that it was sent April 28, 2011 with the subject "Information for Contractor" and "chap6.pdf" attachment:



Information for Contractor
michael.c.campbell

To:	
Sent On:	Thursday, April 28, 2011 8:57:26 AM
Archived On:	Thursday, April 28, 2011 12:58:23 PM
Identification Code:	eml:7527737a-ebf4-4c50-abe7-ad108c032955-2147417640
Attachments:	chap6.pdf (774 KB)

Alcon,

If you have any question, please don't hesitate to contact me.

v/r,

Michael

Figure 1 Screenshot of 4/28/2011 Phish

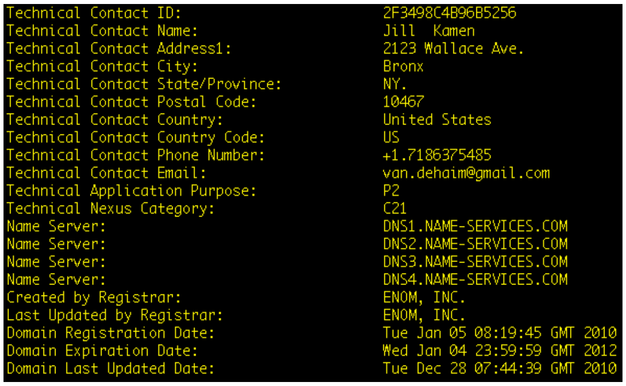
The presentation then goes on to show that opening the PDF attachment exploited a vulnerability and caused a process named "GoogleTray.exe" to launch and connect to:

- mail.hfmforum.com/microsoftupdate/getupdate/default.aspx

Related Backdoor / Beaconing Pattern

By linking domain registration information from some of the C&Cs observed, we were able to determine other C&C domains used by this malicious actor/group. A specific example of this was the following registration information observed in a "MSUpdater" Trojan C&C domain:

[1] http://ilta.ebiz.uapps.net/ProductFiles/productfiles/782804/2011siems.pptx



```
Technical Contact ID:                        2F3498C4B96B5256
Technical Contact Name:                      Jill  Kamen
Technical Contact Address1:                  2123 Wallace Ave.
Technical Contact City:                      Bronx
Technical Contact State/Province:            NY.
Technical Contact Postal Code:               10467
Technical Contact Country:                   United States
Technical Contact Country Code:              US
Technical Contact Phone Number:              +1.7186375485
Technical Contact Email:                     van.dehaim@gmail.com
Technical Application Purpose:               P2
Technical Nexus Category:                    C21
Name Server:                                 DNS1.NAME-SERVICES.COM
Name Server:                                 DNS2.NAME-SERVICES.COM
Name Server:                                 DNS3.NAME-SERVICES.COM
Name Server:                                 DNS4.NAME-SERVICES.COM
Created by Registrar:                        ENOM, INC.
Last Updated by Registrar:                   ENOM, INC.
Domain Registration Date:                    Tue Jan 05 08:19:45 GMT 2010
Domain Expiration Date:                      Wed Jan 04 23:59:59 GMT 2012
Domain Last Updated Date:                    Tue Dec 28 07:44:39 GMT 2010
```

Figure 2 WHOIS information for C&C domains

This contact information was used in other domains that have some open-source reports on C&C usage, for example:

- SISEAU.COM
- VSSIGMA.COM

These domains have open-source reports tied to malware samples with MD5 hashes:

- 3459BC37967480DEE405A5AC678B942D[2]
- 6631815D4AB2A586021C24E02E5CC451[3]

Communication to these domains was also observed with the following C&C communication path pattern:

- /search[RndNum1]?h1=[Num1]&h2=[Num2]&h3=[String1]&h4=[String2]

For example:

- /search521649?h1=51&h2=1&h3=N07630&h4=FKFDFDAHAEBAEPFLFK

The number of parameters in these "search" beacons closely resembles that in the previously mentioned "para" beacons. However, the previously mentioned "para" beacons appear to use a different encoding. These related samples also have VirusTotal reports[4],[5] which provide additional details about the binaries and how they are being detected. Specifically:

[2] http://www.malware-control.com/statics-pages/3459bc37967480dee405a5ac678b942d.php

[3] http://www.threatexpert.com/report.aspx?md5=6631815d4ab2a586021c24e02e5cc451

[4] https://www.virustotal.com/file/6a237ffe0f7d84ffd9652662a2638a9b5212636b414ce15ea2e39204d2a24e7f/analysis/1267308842/

[5] https://www.virustotal.com/file/75d3c3875744196cedff55d179bc62412adeba5e769fbfc85b2b891ff32b4f9f/analysis/1265252262/

MD5: 3459BC37967480DEE405A5AC678B942D

- VirusTotal timeframe: 02/06/2010 – 02/27/2010
- The file name is wuauclt.exe with “Microsoft Corporation” as the publisher (this publisher string was observed in other related samples as well)

MD5: 6631815D4AB2A586021C24E02E5CC451

- VirusTotal timeframe: 08/18/2009 – 02/04/2010
- ThreatExport report shows backdoor on 1033/TCP
- Packed with Armadillo (identified in other related samples as well)

Antivirus detection for both samples indicate that it is a “Backdoor Agent”, however, DrWeb specifically calls these samples something a bit unique: “BackDoor.Calla.5” where “Calla” is the family (added to their detection 02/02/2009)[6] and 5 is the variant.

Searching for other malware / incidents that exhibit this similar “search” / “h1” beaconing pattern shows a number of related open-source examples, as discussed in the following sections.

September 2010 CVE-2010-2883[7] PDF Phish

September 16, 2010 the blog Contagio detailed a malicious phishing campaign exploiting a buffer overflow vulnerability in the Adobe PDF reader[8]. At the time, this was a 0-day exploit, as a patch was not released by Adobe until October 5, 2010. The exploit was contained in the attachment:

- INTEREST_&_FOREIGN_EXCHANGE_RATES.pdf
    - MD5: 4EF704239FA63D1C1DFCF2EA2DA0D711[9]

This PDF dropped a similar set of files:

- setup.exe:
    - MD5: 95D42D365489A6E5EBDF62565C5C8AA2
    - Sophos uniquely detects[10] as Mal/Ovoxual-A (detection added 07/19/2010)[11]
    - Which creates FAVORITES.DAT (data file) and launches msupdater.exe[12]
- msupdater.exe:
    - MD5: 374075CE8B6E8F0CD1F90009FD5A703B

[6] http://vms.drweb.com/virus/?i=225137

[7] http://www.adobe.com/support/security/advisories/apsa10-02.html

[8] http://contagiodump.blogspot.com/2010/09/sep-16-cve-2010-2883-pdf-interest.html

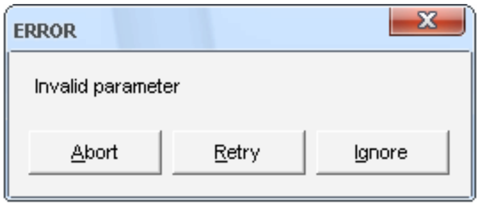
[9] https://www.virustotal.com/file/daac83fc4af5c53068c4e5a29dadfdc5200e3b3fc2b491eebe0a4bc19ec9e3f2/analysis/1285731514/

[10] https://www.virustotal.com/file/ecefcd2f2b862e987ea4b6b7d475c924d9662ad955096872a2c5b822901c63b3/analysis/

[11] http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Mal~Ovoxual-A/detailed-analysis.aspx

[12] http://anubis.iseclab.org/?action=result&task_id=14495366b24a64d242d1946aa1e3a88be&format=html

- ○ Sophos uniquely detects[13] as Mal/ Ovoxual-B (added 07/19/2010)[14]
- ○ Sandbox reports for this sample generally fail[15] showing the following dialog box:



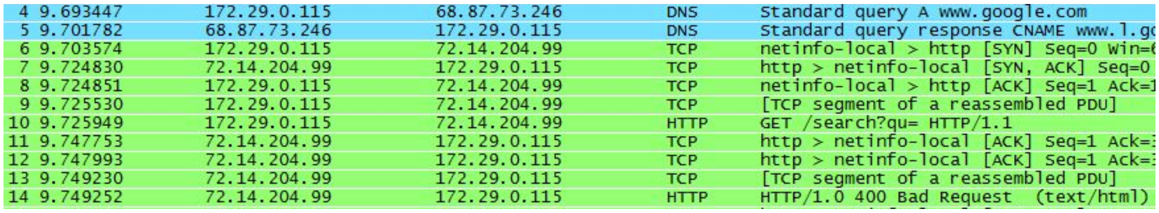
ERROR

Invalid parameter

Figure 3 ThreatExpert Malware Failure Dialog Box

System runtime analysis showed an initial malformed Google query:

- www.google.com/search?qu=



```
 4 9.693447    172.29.0.115    68.87.73.246    DNS    Standard query A www.google.com
 5 9.701782    68.87.73.246    172.29.0.115    DNS    Standard query response CNAME www.l.go
 6 9.703574    172.29.0.115    72.14.204.99    TCP    netinfo-local > http [SYN] Seq=0 Win=6
 7 9.724830    72.14.204.99    172.29.0.115    TCP    http > netinfo-local [SYN, ACK] Seq=0
 8 9.724851    172.29.0.115    72.14.204.99    TCP    netinfo-local > http [ACK] Seq=1 Ack=1
 9 9.725530    172.29.0.115    72.14.204.99    TCP    [TCP segment of a reassembled PDU]
10 9.725949    172.29.0.115    72.14.204.99    HTTP   GET /search?qu= HTTP/1.1
11 9.747753    72.14.204.99    172.29.0.115    TCP    http > netinfo-local [ACK] Seq=1 Ack=
12 9.747993    72.14.204.99    172.29.0.115    TCP    http > netinfo-local [ACK] Seq=1 Ack=
13 9.749230    72.14.204.99    172.29.0.115    TCP    [TCP segment of a reassembled PDU]
14 9.749252    72.14.204.99    172.29.0.115    HTTP   HTTP/1.0 400 Bad Request  (text/html)
```

Figure 4 Malformed Google PCAP During Run-Time Analysis

Followed by failed connection attempts to:

- 140.112.19.195 (National Taiwan University)

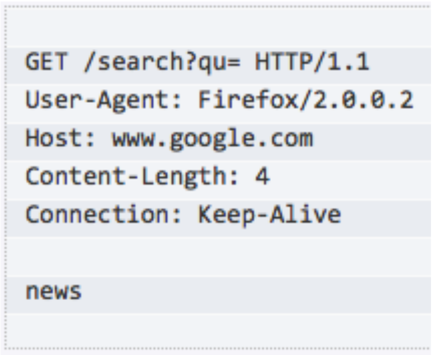
A further detailed static analysis on this msupdate.exe / FAVORITES.DAT sample was completed by CyberESI[16]. In their report they discuss that the setup.exe dropper is virtual machine (VM) aware by using the SIDT instruction[17] – if a VM is detected, the msupdate.exe Trojan is not dropped. The msupdate.exe Trojan too is VM aware using the same SIDT method – if a VM is not detected then the Trojan RC4 decrypts the FAVORITES.DAT file and spawns a svchost.exe process which conducts the network C&C check-ins. This evasion is the reason for the above shown failed sandboxing analysis that does not include any network activity.

The decrypted FAVORITES.DAT executable for this sample had an MD5 hash of:

[13] www.virustotal.com/file-scan/report.html?id=043935374ce39637a4816d0a484d30bed1d3054bbe89625fbc22f83ef4cb3e04-1285736283
[14] http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Mal~Ovoxual-B/detailed-analysis.aspx
[15] http://www.threatexpert.com/report.aspx?md5=374075ce8b6e8f0cd1f90009fd5a703b
[16] http://www.cyberesi.com/2011/03/17/msupdate-exe-favorites-dat-analysis/
[17] http://www.securiteam.com/securityreviews/6Z00H20BQS.html

- 5E3EACA3806769836C3AD9D46A209644[18]
  - Microsoft and a few other A/V vendors detect as Backdoor Matchaldru.B
  - DrWeb uses their same "Calla" family: "Backdoor.Calla.16"
  - The VirusTotal timeframe for submissions of this decrypted executable are from: 03/15/2011 – 04/20/2011.

Here is the Google "decoy beacon" made by the Trojan:

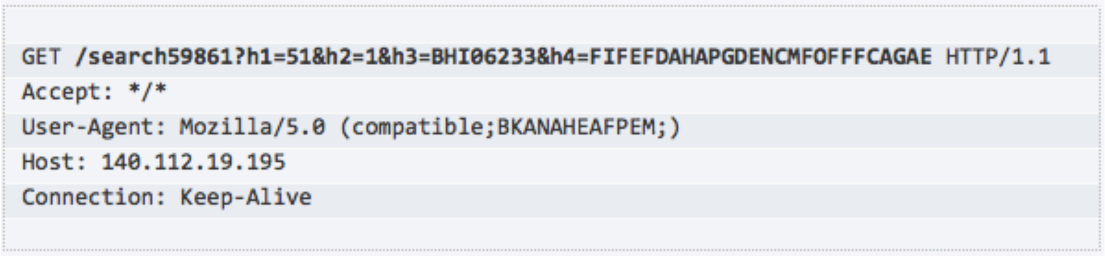


```
GET /search?qu= HTTP/1.1
User-Agent: Firefox/2.0.0.2
Host: www.google.com
Content-Length: 4
Connection: Keep-Alive

news
```

Figure 5 Initial Malformed Google HTTP Request

Followed by the initial C&C check-in request:



```
GET /search59861?h1=51&h2=1&h3=BHI06233&h4=FIFEFDAHAPGDENCMFOFFFCAGAE HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (compatible;BKANAHEAFPEM;)
Host: 140.112.19.195
Connection: Keep-Alive
```

Figure 6 Related Malware C&C Initial Check-In Request

The check-in request values correspond to the following meanings:

- The h1 parameter value corresponds to the Windows version, 51 = Windows XP (version 5.1)
- The h4 parameter value is a victim identification string created by encoding the volume serial number of the victim's system concatenated with a random number
- The string within the user-agent (BKANAHEAFPEM) is the result of an encoding of the victim machine name
- The number following "search5" in the path is random
- The remaining are hard-coded in the Trojan. The "BHI06233" string is thought to be related to the actor's group of related targets or campaign, where BHI may stand for "Baker Hughes

[18] https://www.virustotal.com/file/d8a976979d4eeaf7485249c49d4a31824638a49dac308c5114c113b4a3eed9c9/analysis/1300216834/

International" who along with other companies in the oil, gas, and energy sector were the focus of some targeted attacks.[19]

The data in the check-in HTTP communication to and from the C&C are encoded using single-byte XORing and is treated as authentication into the botnet. Once authenticated, the victim uses the following check-in beacons:

- HTTP GET: /search6[RndNum]?h1=[VictimId]
    - Where VictimId is the same string identifying the victim machine as the previously used h4 parameter value.
- User-Agent: Mozilla/5.0 (compatible; Windows NT 5.2)
    - Note that the user-agent changed to a hard-coded string versus using the encoded system name in the initial check-in.

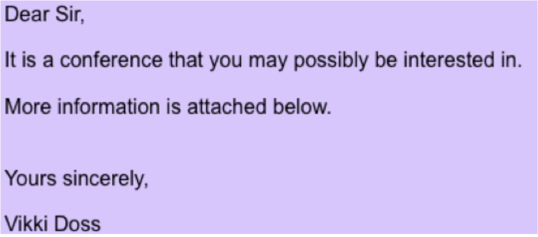
Some of the Trojan functionality includes:

- Download file from C&C:
    - HTTP GET: /download7[RndNum]?h1=[VictimId]
- Upload file to C&C:
    - HTTP POST: /upload8[RndNum]?h1=[VictimId]
- Command execution response to C&C:
    - HTTP POST: /search2[RndNum]?h1=[VictimId]

There are over a dozen other commands identified in the Trojan listed in the CyberESI report.

September 23, 2010 ISSNIP Phishing Email with Malicious Attachment

A few days later following the previously detailed incident, another incident with information publicly available was reported in which a phishing email was sent from a Yahoo account to a defense contractor with content about a conference and malicious attachment, "ISSNIP_2010.pdf" (MD5 hash: 3D966CD90D320EA4A319452D1CCB11AA):



Dear Sir,

It is a conference that you may possibly be interested in.

More information is attached below.

Yours sincerely,

Vikki Doss

Figure 7 Phish Email (9/23/2010)

From the analysis, the malicious attachment appeared to have the same functionality as listed in the previous incident – to include the unique dropped files "msupdater.exe" and "FAVORITES.DAT".

[19] http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-internet-servers.html

Related Antivirus Vendor “Family” Names

In the previously identified samples we have pointed out that certain A/V malware family names are used to identify and classify the fore-mentioned threat. For example,

- DrWeb uses “Backdoor.Calla”
- Microsoft and a few other vendors use “Backdoor.Matchaldru”
- Sophos uses “Mal/ Ovoxual”

Using these identifiers, a number of related samples can be found in the open-source. The following provides a brief list of additional samples believed to be related to this threat group:

- MD5: 92DBDB7E240E7D7C42B4793380782735[20]
  - “msupdate.exe” packed with Armadillo
  - First/Last submitted to VirusTotal: 2011-11-04
  - Sophos identifies as “Mal/Ovoxual-B”
  - McAfee identifies as “Muster.d”
- MD5: 3A0FC856F343B730EE58C00BAB09F9E5[21]
  - “Backdoor.Calla.16”, “Mal/Ovoxual-A”, packed with Armadillo
  - First seen 2010-10-08, Last seen: 2011-03-24
  - Drops[22]:
    - MD5: 7C3C964D7F164F2CC277B41541732546[23]
      - “msupdater.exe”, “Mal/Ovoxual-B”
      - First/Last seen: 2010-09-27
    - MD5: B7424AA1C92107E03DBA8915CEB1FE4D
      - “FAVORITES.DAT” (encrypted)
- MD5: 21816D6934F608E0E3F76AA43831D959[24]
  - “Backdoor.Calla.16”, “Mal/Ovoxual-A”, 2010-10-06
- MD5: 53547213038C093EB427974FA0FB4F65[25]
  - “Mal/Ovoxual-A”, 2010-09-23 – 2011-06-14
- MD5: 0A229293FD0639C722FD7ABD1D1A9C93[26]
  - “Matchaldru.B”, “Mal/Ovoxual-A”, 2011-11-01 – 2011-11-30

From the above VirusTotal results, it appears that McAfee detects some of these as the “Muster” threat group. Using other A/V vendor names and searching and correlating samples in the same way that we did above reveals additional likely related samples. The following provides a brief abbreviated list of samples listed in the open-source for the purposes of showing the breadth of the threat operation timeframe and some PDF names that shed some light on the types of phishing messages used.

[20] https://www.virustotal.com/file/08039422c11ee405af02558704f19c8c53e82749493386a226243ac0f85de20c/analysis/1320449843/
[21] https://www.virustotal.com/file/da3e95eb33c33908ab35b269802ba35fe015e0ad3f0ec7481bcca8b5b96477ca/analysis/
[22] http://www.threatexpert.com/report.aspx?md5=3a0fc856f343b730ee58c00bab09f9e5
[23] https://www.virustotal.com/file/fe0e58b5cad9b1dde19ad87f2470c14879d148c0d271d54e00bb94449a8980fd/analysis/
[24] https://www.virustotal.com/file/d076b318db751cd43e303d26dcaad2d0eab2779185a5facb9aee3754219a322f/analysis/
[25] https://www.virustotal.com/file/5f14bf0b5838f85edcb1bc32a198ec09cf4d73980e73a0783d649e00c91d6771/analysis/
[26] https://www.virustotal.com/file/735fd8ce66e6f0e412f18242d37c12fb38f26f471051eac2f0fe2df89d0e4966/analysis/

- MD5: FD5DFFEBD39E9ACA4F79107B6889699D (09/24/2010)
- MD5: 95AFBECB0BDDE89254DBE07A42685B24 (10/11/2010)
- MD5: 6FF3C8495873AEC4390250EC1ECAA0B1 (04/08/2009)
- MD5: 2EFBF514FBF58E78C259CC87A668BC35 (06/16/2009), drops:
  - MD5: AEDCE18F64EB988F342663EC2C01D017 (COMSWARE_2009.1.pdf)
  - MD5: BDDD2042F5024D2AFC6AA50920E27897 (IEUpd.exe)
  - MD5: EA12A0DBA22B8B2D2D5662437BED8169 (IEXPLORE.hlp)
  - MD5: 7F37F7CD9B0C1CE6574FF5C385FCF26F (WMupdate.exe)
- MD5: 9687E53495898232949DBCD15556B619 (06/16/2009), drops:
  - MD5: 2F71666B76EC0E51A40EF5DF3170604A (2009_IEEE_Aerospace_Conference_1.pdf)
  - MD5: 5622E46F27B8BD7665218E26B024E74D (IEUpd.exe)
  - MD5: D69BB7935DB5FC15542B98845CF83B89 (IEXPLORE.hlp)
  - MD5: A2B6C71A153E61EAA1FEA0F2A3A0232B (WMupdate.exe)
- MD5: 6AD5D9C546AC603E18FC109025E2F5B7 (03/19/2010), drops:
  - MD5: 9C738176C74B7392DD22009736AFC49F (Who will be fired.pdf)
  - MD5: 1ABC034E85704A0699D598B16C16A37E (WMupdate.exe)
- MD5: 7B470C530794342632F5025C1B948BB0 (04/08/2009)
- MD5: 1006e295156b354d9ec4b6d5b6b0ba65 (04/13/2009) drops:
  - MD5: 2F71666B76EC0E51A40EF5DF3170604A (2009_IEEE_Aerospace_Conference_1.pdf)
  - MD5: 9AA8DD1A765C44B82654581977C7F2FA (WMupdate.exe)
- MD5: D78CBD630A1937233B3E4217B19FF5CA (4/13/2009) drops:
  - MD5: BECDA5D5A1C3199A99018A57E43BA2C7 (Bomber_kills_33_at_Iraq_peace_conference.pdf)
  - MD5: 7B470C530794342632F5025C1B948BB0 (WMupdate.exe)
- MD5: 08EB27A6D8F0260D6853BC5A3F5CAA73 (09/15/2009)

“Conference” Lure

As noted in the section on the September 23, 2010 malicious phishing incident, the name of the particular malicious attachment was “ISSNIP_2010.pdf” (see screenshot below) related to the International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)[27]. The use of conference related subjects seems to be the popular lure in this actor’s phishing messages as noted in the above section of related malware. For example;

- IEEE Aerospace Conference
- Iraq Peace Conference
- International Conference on Communication System Software and Middleware (COMSWARE)

[27] http://www.issnip.org

ISSNIP

The Sixth International Conference on Intelligent Sensors, Sensor Networks and Information Processing

ISSNIP 2010 Call for Papers

The Sixth International Conference on Intelligent Sensors, Sensor Networks and Information Processing ISSNIP 2010 (http://www.issnip.org/2010) held under the umbrella of the ARC Research Network on ISSNIP is an annual forum for sensor network research. Recent advances in both theory and applications of intelligent sensors and smart systems in diverse areas ranging from manufacturing and defence to medical science and environmental monitoring will be presented by the leading researchers in the field. The conference will be held in Brisbane, Australia during the 7th-10th of December 2010.

Papers are sought addressing the theory, implementation, and applications of intelligent sensors, sensor networks, and intelligent information processing systems. Topics include:

- Sensor Network Security
- Network Scheduling and Optimization
- Sensor Fusion, Tracking and Localization
- Protocols in Sensor Networks
- Multimedia Sensor Network
- Environmental Monitoring
- Distributed Information Processing
- Data Aggregation, Storage & Management
- Middleware in Sensor Networks
- Fault Tolerance and Identification
- Networked Sensing and Control
- Embedded Software for Sensor Networks
- Energy Efficiency and Management
- Sensor Networks for Smart Grids
- Applications of Sensor Networks in Healthcare, Infrastructure, Defence, Environment

The papers can be nominated under the following symposiums and workshops (see the website for respective details and topic scope).

- Sensor Networks
- Sensor Network Security
- Advances in Optimization for Distributed Control, Information Fusion and Sensor Network Applications
- Sensor Networks for Healthcare
- WSN's for Structural Health Monitoring.
- Cognitive Wireless Sensing Systems for Factory and Logistics Automation
- Smart Cities for Sustainable Living
- ISSNIP/CREON Workshop - Building coral reef sensor networks as systems of systems

Paper Submission:

Prospective authors are invited to submit full papers (up to 6 pages in length) electronically through the EDAS system (http://edas.info/N8697) and must be original material not currently under review by another conference or journal. Author guidelines are available on the conference website. All submitted papers will be subjected to multiple independent peer reviews. All accepted papers will be published by the IEEE Press and appear in the Conference Proceedings and on IEEE Xplore.

Important Dates :
Title and Abstract Submission: **15 August 2010**
Paper Submission: **31 August 2010**
Notification of Acceptance: **30 September 2010**
Final Paper Submission: **7 October 2010**
Conference Dates: **7-10 December 2010**

Contact Information:
ISSNIP 2010
Dept of Electrical and Electronic Engineering,
University of Melbourne, Victoria - 3010, Australia
Email: issnip2010 (at) issnip (dot) org

Technical Co-Sponsorship
IEEE Sensors Council

Sponsors
Australian Government
Australian Research Council

Organised by
ARC Research Network on Intelligent Sensors, Sensor Networks and Information Processing
ISSNIP
THE UNIVERSITY OF MELBOURNE
QUT

General Co-Chairs:
M. Palaniswami, University of Melbourne
Peter Corke, Queensland University of Technology
Slaven Marusic, University of Melbourne

IEEE Sensors Council Liaison:
S C Mukhopadhyay, Massey University

Symposia Chairs/Organizers:
Paul Havinga, University of Twente
Roberto di Pietro, Università di Roma Tre
Yee Wei Law, Uni of Melbourne
Adrian N. Bishop, NICTA
Iman Shames, ANU
Ahsan H. Khandoker, Uni of Melbourne
Daniel T. H. Lai, Victoria University
Rezaul K. Begg, Victoria University
Priyan Mendis, University of Melbourne
Tuan Ngo, University of Melbourne
Laurent Herault, CEA-LETI
Alexander Gluhak, University of Surrey
Srdjan Krco, Ericsson
Sally Holbrook, University of California Santa Barbra
Scott Bainbridge, Australian Institute of Marine Science
Supriyo Chatterjea, University of Twente
Özlem Durmaz İncel, Bogazici University
Raluca Marin-Perianu, Uni of Twente

Publication Chair:
Jayavardhana Gubbi, University of Melbourne

Manuscripts will be made available on
IEEE Xplore RELEASE 2.1

www.issnip.org/2010

Figure 8 ISSNIP 2010 PDF Screenshot

Closing Remarks

Zscaler and Seculert experienced separate security incidents against various customers dealing with a threat appearing to be related to specific targeted attacks. This report provided some insight into the threat and draws in information available in the open-source. In particular, beaconing patterns and indicators were identified to facilitate detection of the threat. Additionally, related malware samples (see Appendix A) and malware family names, such as “Ovoxual”, have been listed for further identification of related samples.

Based on the information available, the threat arrives in phishing emails with a PDF attachment, possibly related to conferences for the particular targeted industry. The PDF exploits vulnerabilities within Adobe (for example, a 0-day exploit was used against CVE-2010-2883) and drops a series of files to begin communicating with the command and control (C&C). The binary dropped and launched from the PDF exploit is virtual machine (VM) aware in order to prevent analysis within a sandbox. If a VM is not detected, it will drop an executable (often named “msupate.exe”), which is also VM aware, and an encrypted file (often named “FAVORITES.DAT”). Again, if no VM is detected this executable will decrypt and run the contents in memory as a process (often the svchost.exe process).

Once the infected system communicates with the C&C, two versions of the beaconing pattern have been observed. The most well documented version of the C&C beaconing adhere to the general formats:

- /search[RndNum]?h1=[Num1]&h2=[Num2]&h3=[String1]&h4=[String2]
- /search[RndNum]?h1=[String1]
- /upload[RndNum]?h1=[String1]
- /download[RndNum]?h1=[String1]

A lesser-known beaconing pattern that both Zscaler and Seculert have observed related to this threat adhere to the general formats:

- /microsoftupdate/getupdate/default.aspx?ID=[num1]para1=[num2]para2=[num3]para3=[num4]
- /microsoft/errorpost/default/connect.aspx?ID=[num1]
- /microsoft/errorpost/default.aspx?ID=[num1]

Prior to beaconing with these patterns the malware may issue an initial malformed Google query:

- GET path: “/search?qu=”
- GET data: “news”

Use these indicators to help provide detection and remediation of this threat within your enterprise. This was the overall goal of releasing this information. Note however, that the overall targeted threat will likely adapt and remain a constant adversary – that is, if your particular organization is the target of an attack it is likely that it will continue to be targeted. Use this knowledge to adapt your organization’s security policies and resources appropriately.

Appendix A: Consolidated List of Malicious MD5 Hashes

The following list is a consolidation of all malicious MD5 hashes listed in this report.

3459BC37967480DEE405A5AC678B942D

6631815D4AB2A586021C24E02E5CC451

3D966CD90D320EA4A319452D1CCB11AA

4EF704239FA63D1C1DFCF2EA2DA0D711

95D42D365489A6E5EBDF62565C5C8AA2

374075CE8B6E8F0CD1F90009FD5A703B

5E3EACA3806769836C3AD9D46A209644

92DBDB7E240E7D7C42B4793380782735

3A0FC856F343B730EE58C00BAB09F9E5

7C3C964D7F164F2CC277B41541732546

B7424AA1C92107E03DBA8915CEB1FE4D

21816D6934F608E0E3F76AA43831D959

53547213038C093EB427974FA0FB4F65

0A229293FD0639C722FD7ABD1D1A9C93

FD5DFFEBD39E9ACA4F79107B6889699D

95AFBECB0BDDE89254DBE07A42685B24

6FF3C8495873AEC4390250EC1ECAA0B1

2EFBF514FBF58E78C259CC87A668BC35

AEDCE18F64EB988F342663EC2C01D017

BDDD2042F5024D2AFC6AA50920E27897

EA12A0DBA22B8B2D2D5662437BED8169

7F37F7CD9B0C1CE6574FF5C385FCF26F

9687E53495898232949DBCD15556B619

2F71666B76EC0E51A40EF5DF3170604A

5622E46F27B8BD7665218E26B024E74D

D69BB7935DB5FC15542B98845CF83B89

A2B6C71A153E61EAA1FEA0F2A3A0232B

6AD5D9C546AC603E18FC109025E2F5B7

9C738176C74B7392DD22009736AFC49F

1ABC034E85704A0699D598B16C16A37E

7B470C530794342632F5025C1B948BB0

1006e295156b354d9ec4b6d5b6b0ba65

2F71666B76EC0E51A40EF5DF3170604A

9AA8DD1A765C44B82654581977C7F2FA

D78CBD630A1937233B3E4217B19FF5CA

BECDA5D5A1C3199A99018A57E43BA2C7

7B470C530794342632F5025C1B948BB0

08EB27A6D8F0260D6853BC5A3F5CAA73