New Poison Ivy Activity Targeting Myanmar, Asian Countries

By Jason Jones on 04/26/2016.
Posted in advanced persistent threats, Backdoors, Malware.

The infamous Remote Access Trojan (RAT) Poison Ivy (hereafter referred to as PIVY) has resurfaced recently, and exhibits some new behaviors. PIVY has been observed targeting a number of Asian countries for various purposes over the past year. Palo Alto Networks' Unit 42 **recently blogged** about a new Poison Ivy variant targeting Hong Kong activists dubbed SPIVY that uses DLL sideloading and operates quite differently from a variant recently observed by ASERT that has been active for at least the past 12 months.

Technical Details

The PIVY variant that ASERT has observed has exhibited some newer behavior that we have not seen discussed previously. The samples drop a decoy doc – usually hinting clearly at the target, a DLL named ActiveUpdate.dll and the PIVY shellcode file as Active.dat. The ActiveUpdate.dll and Active.dat files are created in a directory that follows the format *ActiveUpdate_ [0-9]{3}*. The executable copies rundll32.exe to ActiveFlash.exe and then executes the new file with the path to the DLL and installs itself for automatic startup via a .lnk in the Windows Startup folder. ESET identified these samples as "*Win32/Korplug.I[F-I] variant*", possibly due to the appearance of the malware using DLL sideloading with rundll32 to load the dropped DLL and perform its malicious actions. This deployment tactic dates well into last year (and possibly before) using different executable names for the rundll32 copy and the base directory name, however this post will only cover a subset of the variant using "ActiveUpdate".

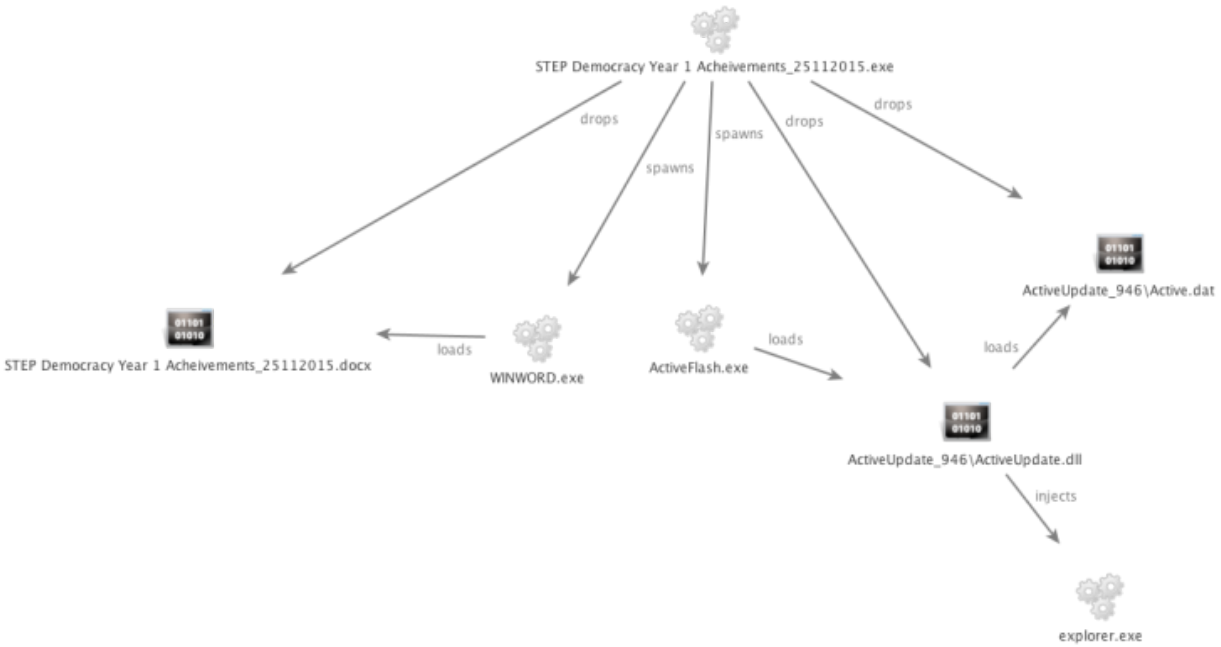


Illustration of execution process of one PIVY Sample

The compile times on these binaries also closely correlate to the times they were first observed in-the-wild and some samples contained timestamp-like entities in the various campaign IDs fields in the malware configuration.

The decrypted configuration appears to be slightly modified in such a way as to confuse some publicly available tools that parse the configuration data. The campaign ID is not fully null-padded – there is now one null-byte and a string of repeating "x" characters that will cause confusion for some scripts. Additionally, the C2s are no longer null-padded – each hostname ends with a null-byte that is then followed by a string that will look something like "0.1127.0.0.1127.0.0.100000". This string will change slightly with each Command & Control (C2) server – the portions that start with "1" will change to 2 for the second C2, 3 for the third, etc. These values end up being present elsewhere in memory without the extra items and only small tweaks are needed to fix the parsing.

The hostname **webserver.servehttp[.]com** is observed in a number of PIVY samples, some of which are covered in this post. Additionally, the IP resolved to by this hostname overlapped with **fileshare.serveftp[.]com** which was used in an earlier and seemingly unrelated PIVY sample.

Decoy Document and Targeting Information

A number of PIVY samples were observed to be targeting Myanmar and several other countries in Asia. While the exact targets and delivery methods are not known to ASERT at this time, the documents and submission sources provide strong hints as to the motivations and potential targets of these exploitation campaigns. The sample described in the previous section – **a7d206791b1cdec616e9b18ae6fa1548ca96a321** –

was observed to be targeting Myanmar in late November 2015. The compile timestamp on the sample was November 2, 2015, the apparent timestamp in the filename appears to be referencing a report that was released on November 25, 2015 and it was first seen late evening in the US on November 24, 2015 which would equate to November 25 in Myanmar. The document was dropped as "***STEP Democracy Year 1 Acheivements_25112015.docx***" and was also dropped by SHA1 **724166261e9c2e7718be22b347671944a1e7fded** with the name "***Year1achievementsv2.docx***", but that sample uses a different communications password over the same set of C2s. The documents may be drafts of a **final report released in December** by the International Institute for Democracy and Electoral Assistance (IDEA), a part of the STEP Democracy initiative. The IDEA is "part of the European Union-funded project *Support to Electoral Processes and Democracy* (STEP Democracy)" whose goal is to support democracy worldwide. The IDEA has been working with Myanmar before and after their recent election to ensure "peaceful, transparent and credible elections." Part of this work includes publishing reports and drafts such as those referenced above. In this case, the bait file document metadata contains a company name of "IDEA" with an author of "Sophia" – possibly referencing a current member of the organization and a last edited date of November 20, 2015. The content of the document details a debate around the democratic elections in Myanmar. This timeline would put the targeting past the elections that occurred in early November, but appears to still be focused on individuals interested in democracy inside of Myanmar. The targeting of the post-election Myanmar appears to be following the same style as what was mentioned in the "**Uncovering the Seven Pointed Dagger**" paper by ASERT. In this case however it appears that threat actors began using references to the STEP organization to continue their likely spearphish tactic by leveraging content relevant to post-election Myanmar. A possible connection exists given that the C2 for these samples – **jackhex.md5c[.]com** – resolved to an IP contained within **103.240.203.0/22** as did a 9002 RAT sample in the Seven Pointed Dagger exploitation campaign. A "LURK0" Gh0strat and another PIVY domain were also observed to have resolved to IPs contained within this range, making this subnet more suspicious from a targeted attack perspective.


STEP DEMOCRACY

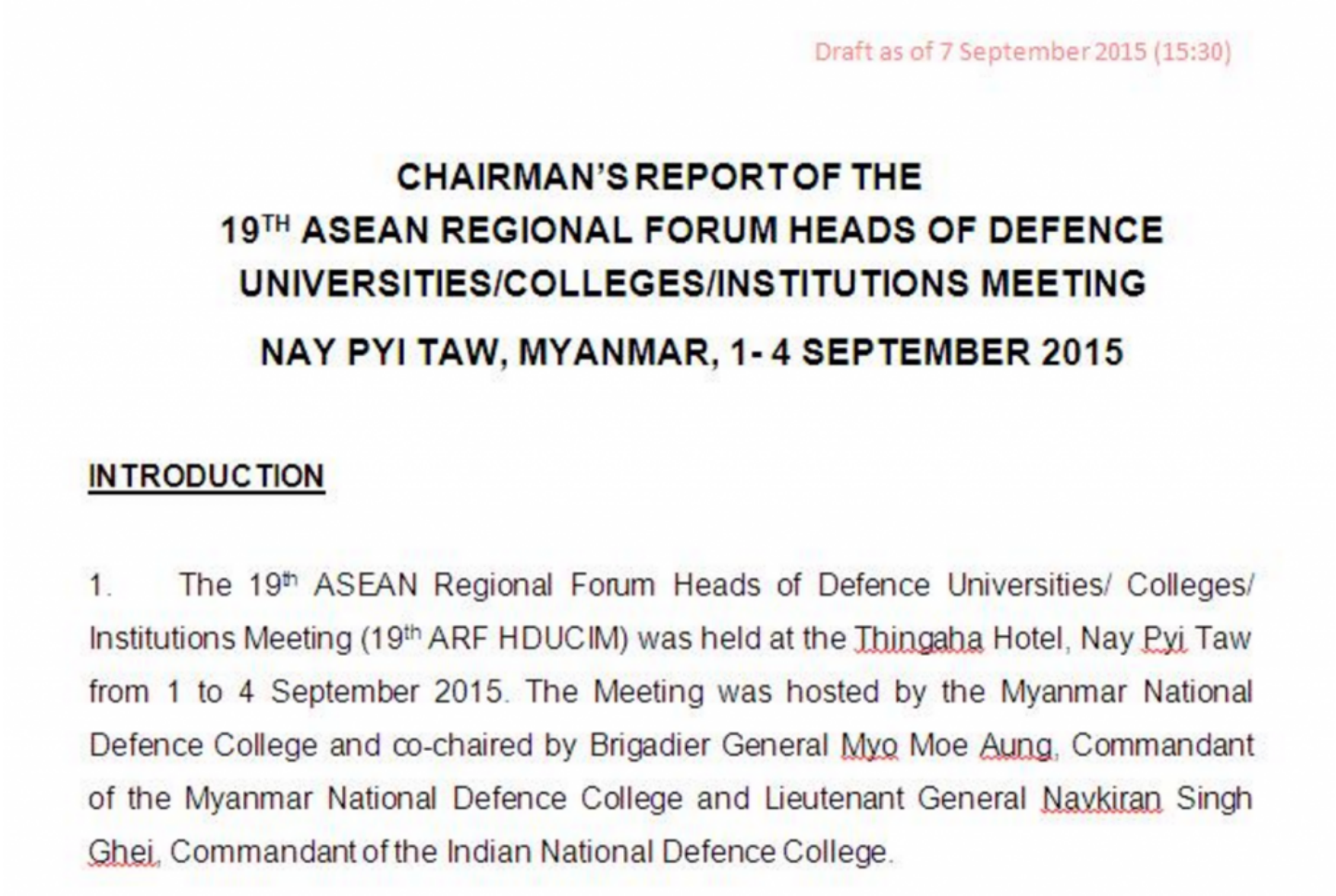
Support to Electoral Processes and Democracy – STEP Democracy

In the first year of a three-year project, Support to Electoral Processes and Democracy (STEP Democracy), made a crucial contribution to the holding of a peaceful, transparent and credible election process. STEP Democracy, supported the Union Election Commission (UEC) in carrying out its operations in a number of areas, including the support to the development of a system to accredit election observers, making the process transparent. Political parties and party agents were trained on essential aspects of the election cycle, and through the establishment of a multi-dialogue platform, supported the endorsement of the Code of Conduct. The programme assisted five Domestic Election Observer groups to implement evidenced-based observation based on international best practice. STEP Democracy enabled civil society leaders to deliver voter education in remote areas of nine States and Regions, reaching directly over 8,500 people.

STEP Democracy have worked together to enhance constructive debate on the political and electoral environment here by regularly providing briefings for Heads of Missions, and in the broader community by hosting a debate held in Myanmar language on Visions for Myanmar's Democratic Future. This event, held on the International Day of Democracy, attracted more than 150 people and press representatives who heard from eminent Myanmar thinkers on this topic.

Dropped document referencing Myanmar's democratic process

A number of documents that appear to be economically focused were also observed recently and one of these samples also references Myanmar. This sample used a campaign ID of "**mm20160405**" and dropped a document named "***Chairman's Report of the 19th ASEAN Regional Forum Heads of Defence Universities, Colleges, Instiutions Meeting, Nay Pay Taw, Myanmar.doc***" that references an Association of Southeast Asian Nations (ASEAN) meeting that took place in Myanmar in September of 2015. The timing of this sample is quite different from the earlier sample and seems to suggest at least a followup campaign due to the malware compilation timestamp of March 28, 2016, combined with an apparent timestamp value in the campaign ID of April 5, 2016 and the fact that the binary was first observed in the wild on April 11, 2016. The mutex specified in the configuration – **20150120** – is the same mutex used in the earlier sample that dropped a document referencing the STEP program, but this mutex is also used in many other PIVY samples that use the "ActiveUpdate" directory structure and is likely not useful for identifying the campaign or a relationship between samples outside of possibly sharing a similar version. The C2 used in this sample – **admin.nslookupdns[.]com** – resolved to an IP contained in the subnet **118.193.218.0/24**. Similar to the previous sample discussed, ASERT has observed an overlap between many other malware families including Nitol, Gh0strat, and another PIVY sample that uses "**ActiveUpdate**". This sample's C2 domain is **news.tibetgroupworks[.]com** which provides an obvious suggestion at targeting dynamics, however no decoy documents were dropped and no further information was discovered to help support the targeting hypothesis.



Draft as of 7 September 2015 (15:30)

CHAIRMAN'S REPORT OF THE
19TH ASEAN REGIONAL FORUM HEADS OF DEFENCE
UNIVERSITIES/COLLEGES/INSTITUTIONS MEETING
NAY PYI TAW, MYANMAR, 1- 4 SEPTEMBER 2015

INTRODUCTION

1. The 19th ASEAN Regional Forum Heads of Defence Universities/ Colleges/ Institutions Meeting (19th ARF HDUCIM) was held at the Thingaha Hotel, Nay Pyi Taw from 1 to 4 September 2015. The Meeting was hosted by the Myanmar National Defence College and co-chaired by Brigadier General Myo Moe Aung, Commandant of the Myanmar National Defence College and Lieutenant General Navkiran Singh Ghei, Commandant of the Indian National Defence College.

Dropped document referencing ASEAN meeting in Myanmar

Continuing on with the theme of campaigns targeting ASEAN, sample **31756ccdbfe05d0a510d2dcf207fdef5287de285** drops a decoy document named "***Robertus Subono-REGISTRATION_FORM_ASEAN_CMCoord2016.docx***" that references an ASEAN Humanitarian Civil Military Coordination meeting that took place in Bangkok between March 28 and April 1 2016. The document purports to be a registration form for an attendee from Indonesia and is supposed to be sent to a Thailand Ministry of Defense email address. The sample has a compilation date of March 10, 2016, was first observed by ASERT on March 20, 2016 and also contains an invalid digital signature claiming to be signed by Google. Coupling the campaign ID of "**modth**" with the purpose and location of the meeting and the email address this form is supposed to be mailed to, a possible target of this sample could be Thailand's Ministry of Defense. The C2s used by this sample overlap with the prior sample that references the ASEAN meeting in Myanmar nearly perfectly – the first C2 uses port 80, whereas the prior sample used 81 and they both use the same mutex and password. This overlap suggests a possible ongoing targeting towards ASEAN members and meetings that they hold.

ASEAN CMCoord 2016

ASEAN Humanitarian Civil Military Coordination Workshop 2016

28 March - 1 April 2016, Royal Orchid Sheraton, Bangkok, Thailand

REGISTRATION FORM for *Delegation*

Thank you for registering for "ASEAN Humanitarian Civil Military Coordination 2016 (ASEAN CMCoord 2016). Please print or type clearly and return the completed form to disaster@mod.go.th Tel. + 66 2 622-3606 or + 66 2 224-2032 by **Friday 4 March 2016** (**PLEASE COMPLETE THIS FORM BY USING BLOCK LETTERS**)

PERSONAL INFORMATION		
Country	INDONESIA	
Title	✓ MR ☐MS ☐Other ( )	
Name	**First Name**	ROBERTUS
	Middle Name	
	Last Name	SUBONO
	Name Tag Information	ROBERTUS SUBONO

Decoy document dropped by 31756ccdbfe05d0a510d2dcf207fdef5287de285 referencing an ASEAN meeting in Thailand

The decoy document "***2016.02.29-03.04 -ASEM Weekly.docx***" dropped by **ec646c57f9ac5e56230a17aeca6523a4532ff472** was also interesting in that it was not in English like the other two observed documents – Google Translate identifies the language in the document as Mongolian.

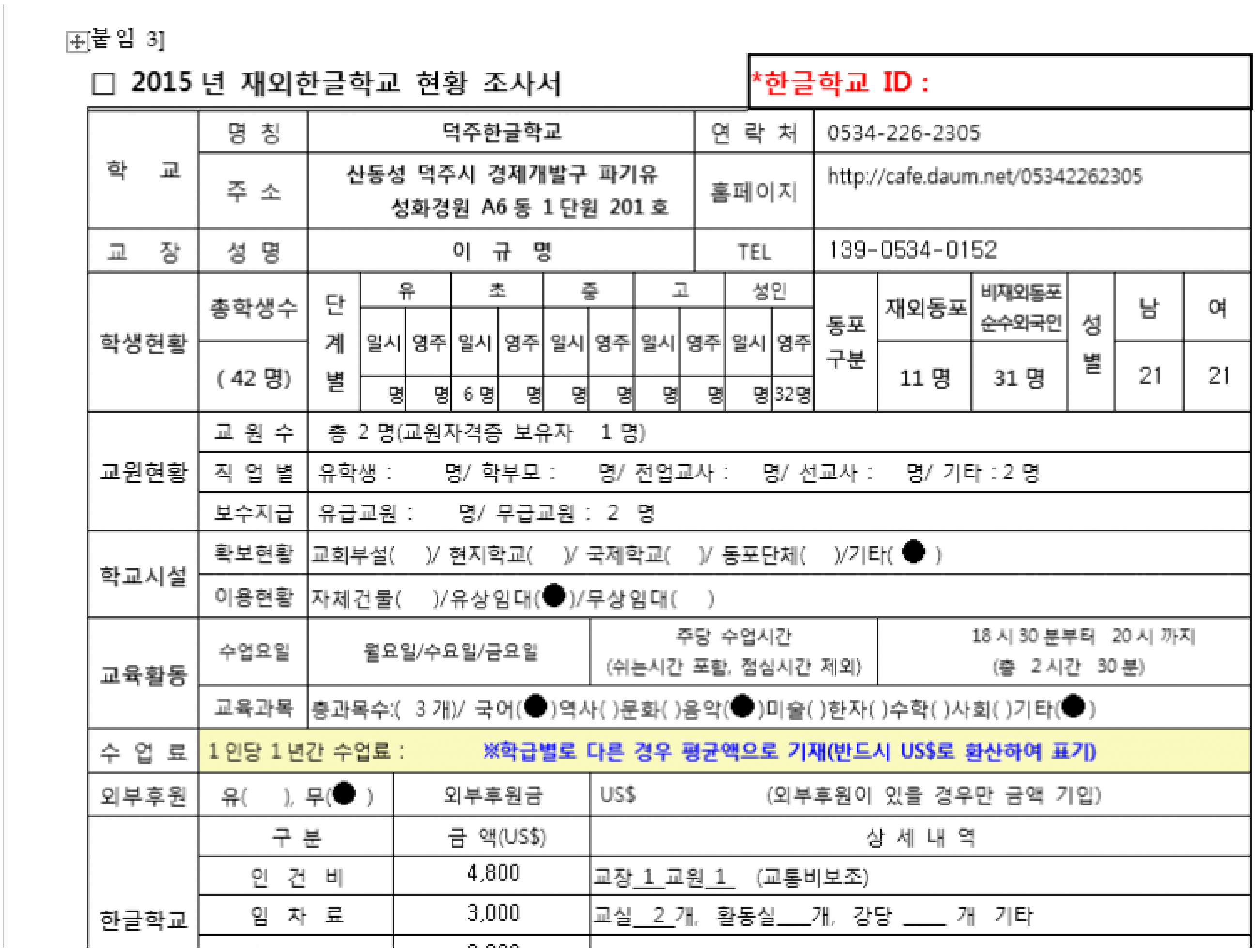
МОНГОЛ УЛСЫН ГАДААД ХЭРГИЙН ЯАМ
АСЕМ-ЫН БЭЛТГЭЛ АЖЛЫН АЛБА
ДОЛОО ХОНОГИЙН АЖЛЫН ТОЙМ
/2016.02.29- 03.04/

Хийж гүйцэтгэсэн ажлууд:

- АСЕМ-ын бэлтгэл ажилтай танилцахаар ХБНГУ-аас ирсэн урьдчилсан багийг хүлээн авч, холбогдох газруудтай хийсэн уулзалтуудыг зохион байгуулав.
- Үндэсний Зөвлөлийн 16 дугаар хуралдаанаар АСЕМ-ын Дээд түвшний уулзалтын зочдод үйлчлэх автомашины санхүүжилт, ИНЕГ болон МИАТ компанийн шаардлагатай санхүүжилтийн асуудлуудыг хэлэлцүүлэв.
- Ази, Европын Дээд түвшний 11 дүгээр уулзалтын зохион байгуулалтад дэмжлэг үзүүлэх олон нийтийн оролцоог дэмжих зорилготой Хандивын хүлээн авалтын бэлтгэл ажлыг ханган ажиллаж байна.
- Улаанбаатар хотноо 2 дугаар сарын 23-25-ны өдрүүдэд ирж ажилласан ЕХ-ны Гадаад харилцааны албаны АСЕМ-ын асуудал хариуцсан Ерөнхий зөвлөх Майкл Маттисон тэргүүтэй албаны төлөөлөгчдийн

Decoy document references an Asia-Europe Meeting (ASEM) dropped by ec646c57f9ac5e56230a17aeca6523a4532ff472

The decoy document ***1.docx*** that is dropped by **f389e1c970b2ca28112a30a8cfef1f3973fa82ea** shows as corrupted when executed in a sandbox, but manual recovery yielded a document in Korean with a malware campaign ID of **kk31**. The document appears to reference Korean language schools abroad and the telephone number present yields an affiliation with the Korean Ministry of Foreign Affairs, but the intended target is unclear at this time.



[붙임 3]

☐ 2015 년 재외한글학교 현황 조사서 *한글학교 ID :

학 교	명 칭	덕주한글학교	연 락 처	0534-226-2305
	주 소	산동성 덕주시 경제개발구 파기유 성화경원 A6 동 1 단원 201 호	홈페이지	http://cafe.daum.net/05342262305
교 장	성 명	이 규 명	TEL	139-0534-0152

			유		초		중		고		성인			재외동포	비재외동포 순수외국인		남	여
학생현황	총학생수	단계별	일시	영주	일시	영주	일시	영주	일시	영주	일시	영주	동포구분			성별		
	(42 명)		명	명	6 명	명	명	명	명	명	명	32명		11 명	31 명		21	21

교원현황	교 원 수	총 2 명(교원자격증 보유자 1 명)
	직 업 별	유학생 : 명/ 학부모 : 명/ 전업교사 : 명/ 선교사 : 명/ 기타 : 2 명
	보수지급	유급교원 : 명/ 무급교원 : 2 명
학교시설	확보현황	교회부설( )/ 현지학교( )/ 국제학교( )/ 동포단체( )/기타(●)
	이용현황	자체건물( )/유상임대(●)/무상임대( )
교육활동	수업요일	월요일/수요일/금요일 / 주당 수업시간 (쉬는시간 포함, 점심시간 제외) / 18 시 30 분부터 20 시 까지 (총 2 시간 30 분)
	교육과목	총과목수:(3 개)/ 국어(●)역사( )문화( )음악(●)미술( )한자( )수학( )사회( )기타(●)
수 업 료	1 인당 1 년간 수업료 : ※학급별로 다른 경우 평균액으로 기재(반드시 US$로 환산하여 표기)	
외부후원	유( ), 무(●) / 외부후원금	US$ (외부후원이 있을 경우만 금액 기입)

	구 분	금 액(US$)	상 세 내 역
한글학교	인 건 비	4,800	교장 1 교원 1 (교통비보조)
	임 차 료	3,000	교실 2 개, 활동실___개, 강당 ____ 개 기타

Korean language decoy document dropped by

Sample **f389e1c970b2ca28112a30a8cfef1f3973fa82ea** dropped a decoy document named "***Commission on Filipinos Overseas & Dubai.doc***", but this document did not render correctly in a malware sandbox or manually. VirusTotal revealed a sample from the Philippines which suggests that they, not Dubai / UAE, were the targets. The C2s for this sample used **webserver.servehttp[.]com**, also exhibited by many of the recent samples which suggests the same actor may be involved in this campaign activity.

Conclusion

As this post and other recent posts detail, PIVY continues to evolve and be used in a myriad of targeted exploitation campaigns – not unlike many other targeted malware families such as PlugX or the Dukes. This will certainly not be the last evolution of PIVY, and ASERT continues to monitor these threats as they are discovered. I would also like to say thank you to **Curt Wilson** of ASERT for his assistance with research covered in this post.

IOCS

Configuration elements and additional information for samples discussed in this article.

SHA1: a7d206791b1cdec616e9b18ae6fa1548ca96a321
First Seen: Nov. 24, 2015
Name:STEP Democracy Year 1 Acheivements_25112015.exe
Decoy Doc: STEP Democracy Year 1 Acheivements_25112015.docx
Campaign ID: om
C2s: jackhex.md5c.net:8080
    jackhex.md5c.net:53
    jackhex.md5c.net:53
Mutex: 20150120
Password: 18703983384

SHA1: 724166261e9c2e7718be22b347671944a1e7fded
First Seen: Nov. 23, 2015
Name:Year1achievementsv2.exe
Decoy Doc: Year1achievementsv2.docx
Campaign ID: om
C2s: jackhex.md5c.net:8080
    jackhex.md5c.net:53
    jackhex.md5c.net:53
Mutex: 20150120
Password: 15911117665

SHA1: 675a3247f4c0e1105a41c685f4c2fb606e5b1eac
First Seen: April 7, 2016
Name: Commission on Filipinos Overseas & Dubai %E2%80%AEcod.doc
Decoy Doc: Commission on Filipinos Overseas & Dubai.doc
Campaign ID: gmkill
C2s: webserver.servehttp.com:8080
    webserver.servehttp.com:8080
    webserver.servehttp.com:8081
Mutex: 20150120
Password: 13813819438

SHA1: 63e00dbf45961ad11bd1eb55dff9c2771c2916a6
First Seen: April 11, 2016
Name: 1.exe
Decoy Doc: Chairman's Report of the 19th ASEAN Regional Forum Heads of Defence Universitie
Campaign ID: mm20160405
Domain Created: December 17, 2015
C2s: admin.nslookupdns.com:81
    admin.nslookupdns.com:53
    admin.nslookupdns.com:8080
Mutex: 20150120
Password: 52100521000

SHA1: 31756ccdbfe05d0a510d2dcf207fdef5287de285
First Seen: March 20, 2016
Name: Unknown
Decoy Doc: Robertus Subono-REGISTRATION_FORM_ASEAN_CMCoord2016.docx
Campaign ID: modth
Domain Created: December 17, 2015
C2s: admin.nslookupdns.com:80
    admin.nslookupdns.com:53
    admin.nslookupdns.com:8080

```
Mutex:  20150120
Password: 52100521000

SHA1: ec646c57f9ac5e56230a17aeca6523a4532ff472
First Seen: March 10, 2016
Name: 2016.02.29-03.04 -ASEM Weekly.docx.rar^2016.02.29-03.04 -ASEM Weekly.docx.exe
Decoy Doc: 2016.02.29-03.04 -ASEM Weekly.docx (Mongolian language)
Campaign ID: wj201603
Domain Created: January 14, 2016
C2s:    web.microsoftdefence.com:8080
    web.microsoftdefence.com:8080
    web.microsoftdefence.com:80
Mutex: 20150120
Password: 80012345678

SHA1: f389e1c970b2ca28112a30a8cfef1f3973fa82ea
Name: Unknown
Decoy Doc: 1.docx (corrupted but recoverable, Korean language)
First Seen: April 9, 2016
CampaignID: kk31
C2s:    webserver.servehttp.com:59148
    webserver.servehttp.com:59418
    webserver.servehttp.com:5000
Mutex: 20160301
Password: 13177776666

SHA1: 49e36de6d757ca44c43d5670d497bd8738c1d2a4
Name: Unknown
Decoy doc: 1.pdf, references project in Vietnam requesting an email to a Thailand email ac
First Seen: March 10, 2016
C2s:    webserver.servehttp.com:59148
        webserver.servehttp.com:59418
        webserver.servehttp.com:1024
Mutex: 20160219
Campaign ID: mt39

Discovered during investigation, but do not drop decoy docs, exhibited similar configurati
SHA1: ef2618d58bd50fa232a19f9bcf3983d1e2dff266
Name: 2.tmp
Decoy Doc: None
First Seen: June 3, 2015
Domain Created: May 29, 2015
C2s:    news.tibetgroupworks.com:80
    news.tibetgroupworks.com:80
    news.tibetgroupworks.com:80
Campaign ID: 213
Mutex: 2015012
```

SHA1 Hashes

63e00dbf45961ad11bd1eb55dff9c2771c2916a6
675a3247f4c0e1105a41c685f4c2fb606e5b1eac
49e36de6d757ca44c43d5670d497bd8738c1d2a4
cbbfc3b5ff08de14fdb2316f3b14886dfe5504ef
a7d206791b1cdec616e9b18ae6fa1548ca96a321
ec646c57f9ac5e56230a17aeca6523a4532ff472
ef2618d58bd50fa232a19f9bcf3983d1e2dff266
f389e1c970b2ca28112a30a8cfef1f3973fa82ea

Unique C2 Hostnames

news.tibetgroupworks.com
web.microsoftdefence.com
admin.nslookupdns.com
jackhex.md5c.net
webserver.servehttp.com

Arbor's Security Engineering & Response Team (ASERT) delivers world-class network security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions

that are referred to as ‘super remediators’ and represent the best in information security. ASERT has both visibility and remediation capabilities at nearly every tier one operator and a majority of service provider networks globally.

ASERT shares operationally viable intelligence with hundreds of international Computer Emergency Response Teams (CERTs) and with thousands of network operators via in-band security content feeds. ASERT also operates the world’s largest distributed honeynet, actively monitoring Internet threats around the clock and around the globe via ATLAS®, Arbor’s global network of sensors: http://atlas.arbor.net.

TAG CLOUD

Black Peace Group Attacks algorithm Aldi 504 traffic network Iran Internet Protocol hijack Facebook Dirt Jumper Danny McPherson China Bot Wikileaks IPv6 Armageddon YouTube Security Botnet Internet service provider Internet traffic Google outage Arbor Networks - DDoS Experts BGP peering "End of Internet" Botnets Crypto Denial-of-service attack down Halloween internet IPv4 malware Streaming media 500 Internal DDoS AlbaDDoS Aldi Bot attack Beer DDoS Blog