

RSA[®]Conference2017

Singapore | 26–28 July | Marina Bay Sands

POWER OF
OPPORTUNITY

SESSION ID: TTA-R01

APT Attacks in the Asia Pacific



Sean Duca

Chief Security Officer – APAC
Palo Alto Networks
@seanduca



Vicky Ray

UNIT 42 – Threat Intelligence Analyst
Palo Alto Networks
@0xVK

AGENDA

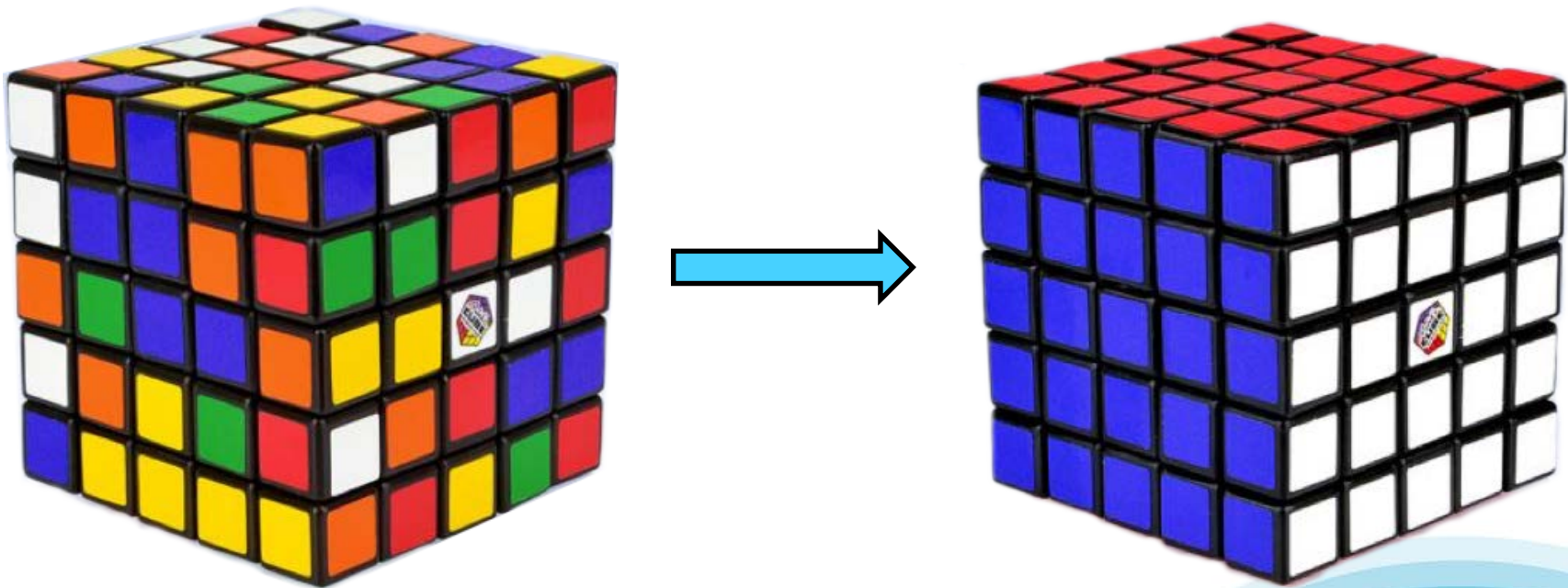
- Unit 42 Mission
- Why Asia Pacific is a constant target of APT threat actors
- 0-days or known exploits
- Targeted Attack Case studies
- What do we learn from the APT attacks
- Way forward

Unit 42 Mission



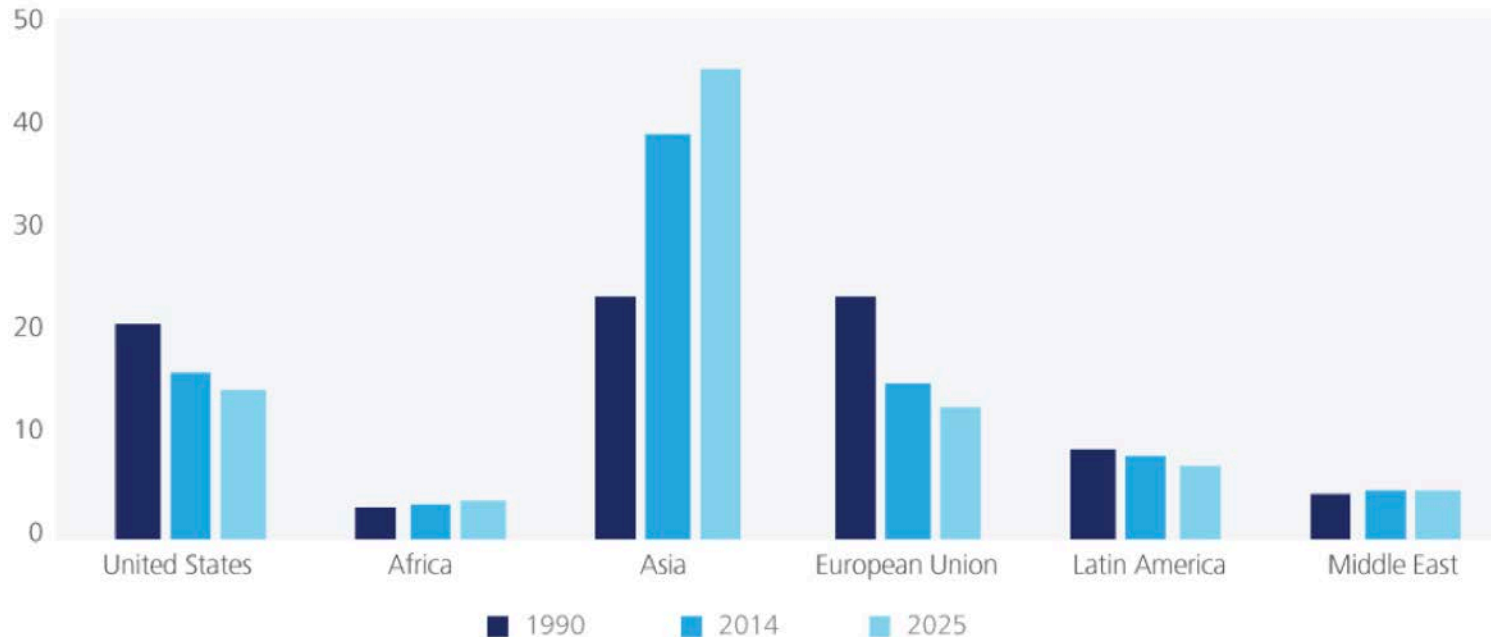
Analyze the data available to Palo Alto Networks to identify adversaries, their motivations, resources, and tactics to better understand the threats our customers face.

Connecting the dots together



Why is Asia Pacific a target of APT ?

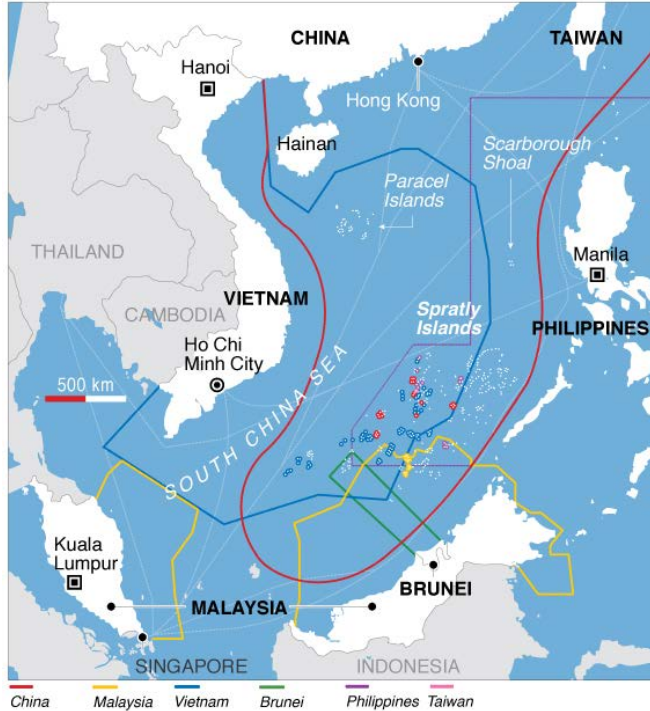
Figure 2. Asia's share (percentage) in global GDP (real US\$ PPP) will increase further



Source: Oxford Economics, Deloitte Services LP economic analysis.
Forecasts are by Oxford Economics.

Graphic: Deloitte University Press | DUPress.com

Why is Asia Pacific a target of APT ?



https://en.wikipedia.org/wiki/Territorial_disputes_in_the_South_China_Sea



Territorial disputes

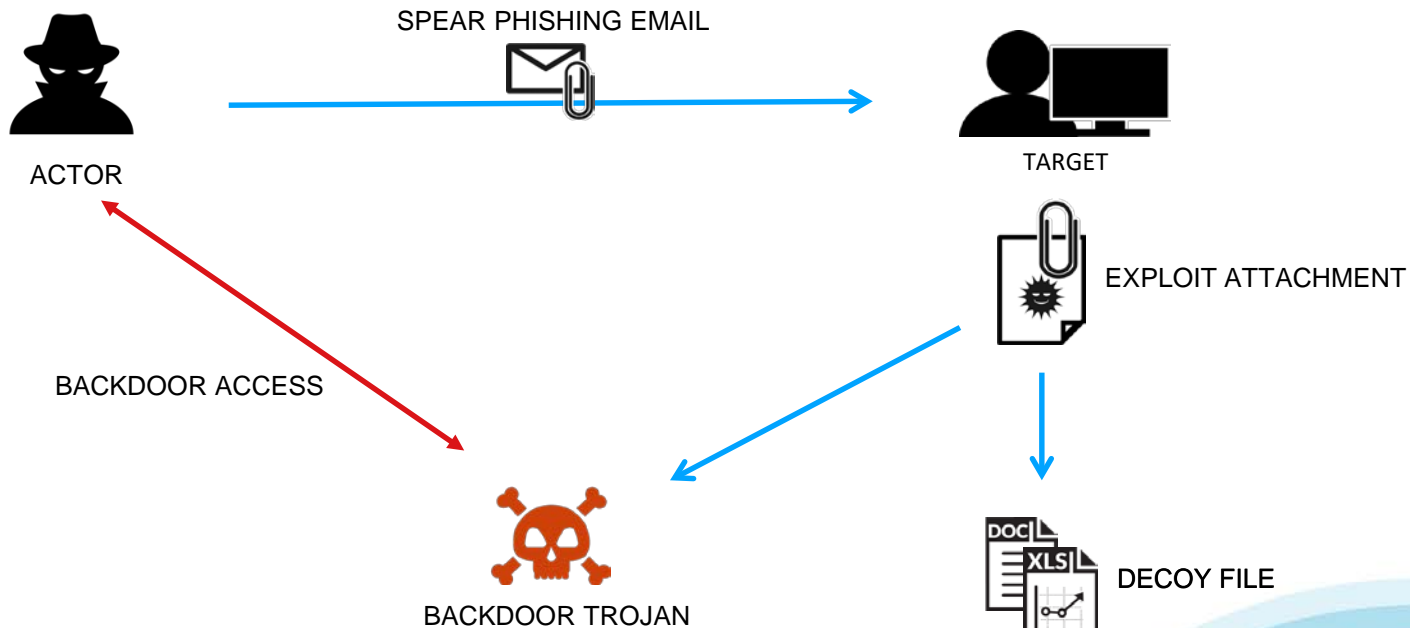
Most Targeted Application ?



Zero-days or Known exploits used

- CVE-2010-3333 — Microsoft Office Remote Code Execution Vulnerability
- CVE-2012-0158 — Microsoft Office Remote Code Execution Vulnerability
- CVE-2017-0199 — Microsoft Office/WordPad Remote Code Execution Vulnerability.

SPEAR PHISHING + DECOY

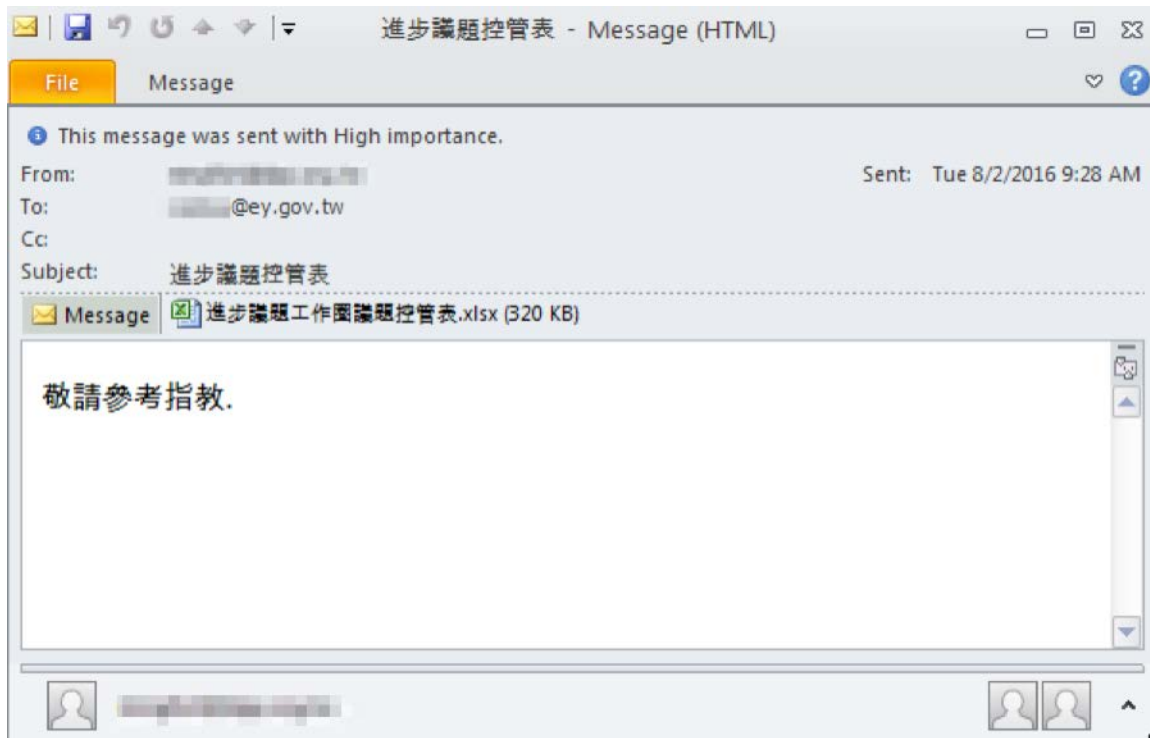


TROPIC TROOPER targets
the Taiwan Government



Who is Tropic Trooper?

TROPIC TROOPER TARGETS THE TAIWAN GOVERNMENT



TARGETED SPEAR-PHISHING
EMAIL WAS SENT TO THE
SECRETARY GENERAL OF
EXECUTIVE YUAN, TAIWAN
GOVERNMENT

DECOY USED BY TROPIC TROOPER

B37		
A	B	C
1 負責人	議題概要及主要團體	動態發展重點
2	<p>2015秋門--</p> <p>揭穿右派假進步，左翼奮起要真權集合時間：11月22日下午一時</p> <p>集合地點：凱達格蘭大道</p> <p>遊行終點：蔡英文競選總部</p> <p>門陣團體：台灣高等教育產業工會、桃園在地聯盟、全國教師工會總聯合會、工作傷害受害人協會、桃園市教育產業工會、工人國際委員會、媒體改造學社、青年勞動九五聯盟、紀錄片工會、高雄市教育產業工會</p>	<p>1.其中工鬥五大政策訴求經工鬥國是會議後較為明確：1.年金保障；2.長照安養；3.醫消護勞動條件4.總罷工解禁；5.約聘僱檢討</p> <p>2.台灣國際勞工協會擬於11/24拜會本黨，並就工鬥國是會議中，長照政策相關之議題，與本黨交換意見。</p>
3	馬習會	<p>1.自台黨：預計明日赴立院，軟性抗議毛治國報告馬習會</p> <p>2.基進側翼：錄製網路宣傳短片，分析馬習會影響 吳清彥等人：已返抵台灣</p> <p>3.綠社聯盟、時代力量：將馬習會連結至國會選舉時代力量與綠社聯盟，於起訴點各</p>
鍾和旺	<p>台中/大度山敬啟一、主要推動團體與個人：台灣護樹團體聯盟、台灣護樹協會、搶救大肚山反中科擴廠自救會、主婦聯盟台中分會、</p>	<p>一、2015.11.28中科擴廠停工大遊行</p> <p>本次遊行訴求：</p> <p>1.</p>

DECOY USED IN THE ATTACK
AGAINST THE SECRETARY
GENERAL OF EXECUTIVE YUAN,
TAIWAN GOVERNMENT

▶	範例	0720	0721	1041109全更新
---	----	------	------	------------

TROPIC TROOPER PAYLOAD EXTRACTED AFTER DECRYPTION

	Key	Ciphertext	Cleartext
0	$\sim 0x45218 = 0xFFFBAD E8 \gg 1 = 0x7FFDD6F4$	0x7F6D8CB9	0x00905a4d = MZ\x90\x00
1	$0x7FFDD6F4 \gg 1 = 0x3FFE EB7A$	0x3FFE EB79	0x03 = \x03\x00\x00\x00
2	$0x3FFE EB7A \gg 1 = 0x1FFF75BD$	0x1FFF75B9	0x04 = \x04\x00\x00\x00
3	$0x1FFF75BD \gg 1 = 0x8FFFBADE$	0x8FFF4521	0xFFFF = \xff\xff\x00\x00

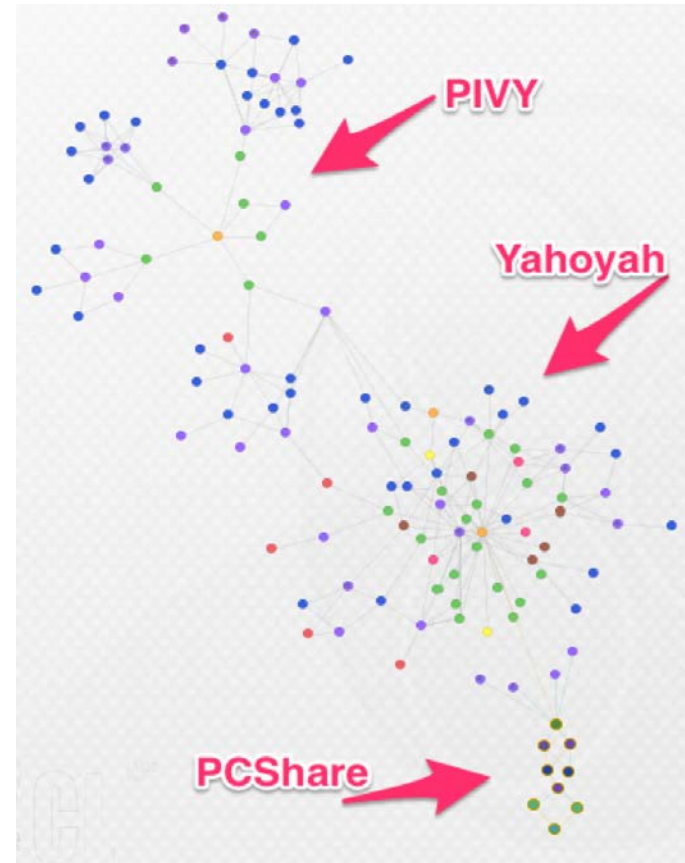
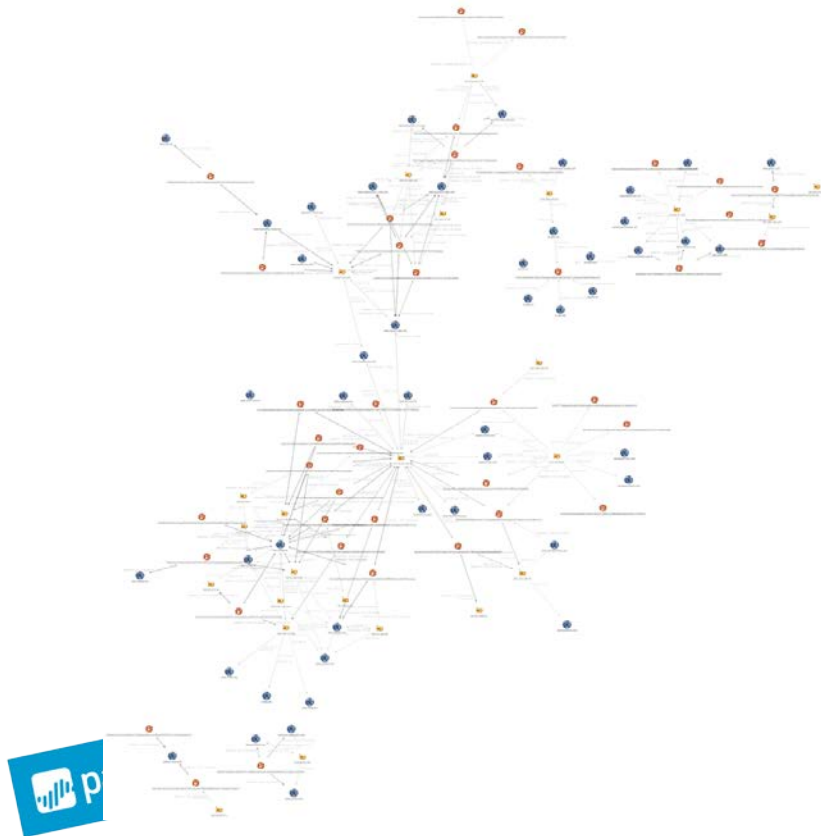
HIDDEN PAYLOAD EXTRACTED
AFTER DECRYPTION

19	$0x75BD1FFF \gg 1 = 0xBADE8FFF$	0xD28AAE32	0x685421CD = \xcd!Th
20	$0xBADE8FFF \gg 1 = 0xDD6F47FF$	0xAD4F3496	0x70207369 = is p
21	$0xDD6F47FF \gg 1 = 0xEEB7A3FF$	0x9CD0CC8D	0x72676F72 = rogr
22	$0xEEB7A3FF \gg 1 = 0xF75BD1FF$	0x947BBC9E	0x63206D61 = am c
23	$0xF75BD1FF \gg 1 = 0xFBADE8FF$	0x94C3869E	0x6F6E6E61 = anno
24	$0xFBADE8FF \gg 1 = 0xFDD6F47F$	0x98B4D40B	0x65622074 = t be
25	$0xFDD6F47F \gg 1 = 0xFFEEB7A3F$	0x909E081F	0x6E757220 = run

EXPLOIT & MALWARE USED

- Exploit - CVE-2012-0158 (no surprises)
- Malware – Trojan : Poison Ivy
- Investigations on related infrastructure provided details of other tools being used by Tropic Trooper
 - Yahoyah
 - PCshare

INFRASTRUCTURE AND ASSOCIATED MALWARE



NEW DECOYS USED IN RECENT SAMPLES SUGGEST TARGETS IN VIETNAM

A1		CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
		A
1		CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
2		Độc lập - Tự do - Hạnh phúc
3		
4		SƠ YẾU LÝ LỊCH TỰ THUẬT
5		
6	Họ và tên:	Lê Trọng Nghĩa Sinh ngày:24/04/1990 Nam/ Nữ: Nam
7	Dân tộc:	Kinh Tôn giáo:Không Ngày nhập ngũ (Ký HQLĐ):
8	Cấp bậc:Chức vụ:.....
9	Đơn vị công tác:	Phòng QTHT. Trung tâm CNTT-VTNet
10	Số CMT:	168348853 Ngày cấp:29/12/2007 Nơi cấp: Hà Nam
11	Ngày vào Đảng (Đoàn):	Đoàn: 26/03/2013 Chính thức:
12	Trình độ văn hóa:	12/12 Chuyên môn nghiệp vụ: CNTT
13	Quê quán:	Thị Trấn Quế- Kim Bảng- Hà Nam
14	Chỗ ở hiện nay:	Tây Mỗ- Từ Liêm- Hà Nội
15	TÌNH HÌNH KINH TẾ - CHÍNH TRỊ - XÃ HỘI CỦA GIA ĐÌNH	
16		
17	Bố đẻ:	Lê Ngọc Sơn Sinh năm: 1961 Nghề nghiệp: Công chức xã
18	Quê quán:	Thị Trấn Quế- Kim Bảng- Hà Nam
19	Nơi ở hiện nay:	Thị Trấn Quế- Kim Bảng- Hà Nam
20	Nơi công tác:	UBND Thị Trấn Quế- Kim Bảng- Hà Nam
21	Thái độ chính trị từ trước đến nay làm gì cho cách mạng, cho chế độ cũ (yêu cầu ghi rõ thời gian tham gia, cấp I	

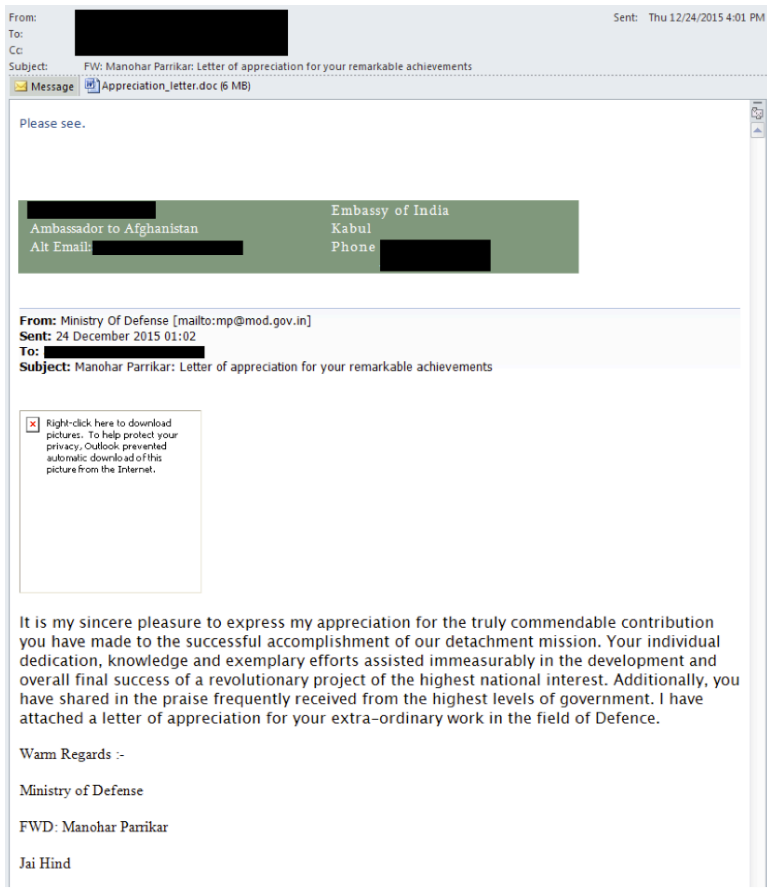
Recent samples show that the targets are in Vietnam too

Payload dropped : Pivy
Shares same mutex

Malware ROVER used to
Target the Indian Ambassador
To Afghanistan

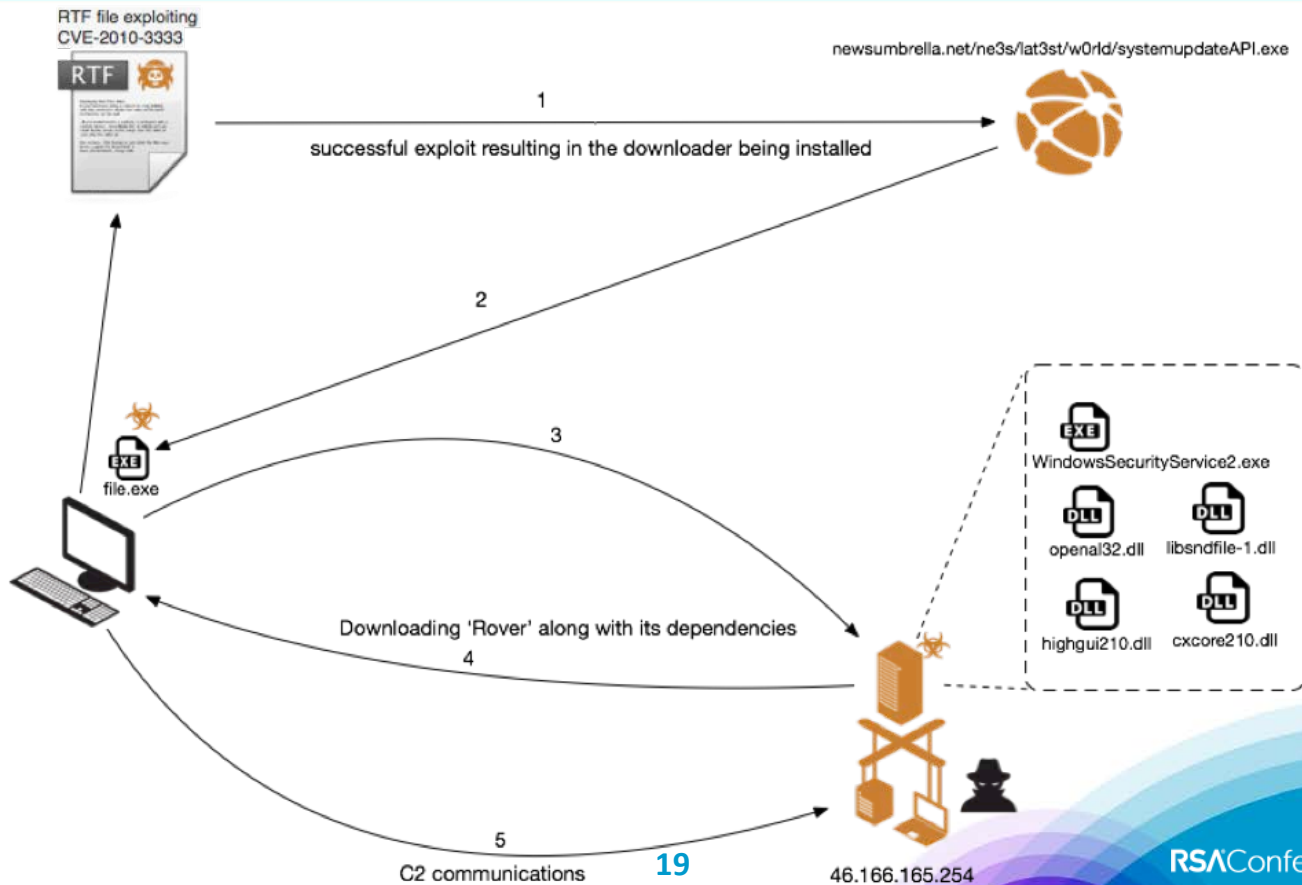


SPEAR-PHISHING EMAIL



TARGETED SPEAR-PHISHING
EMAIL WAS SENT TO THE
AMBASSADOR OF INDIA TO
AFGHANISTAN

INFECTION FLOW



BACKDOOR COMMANDS

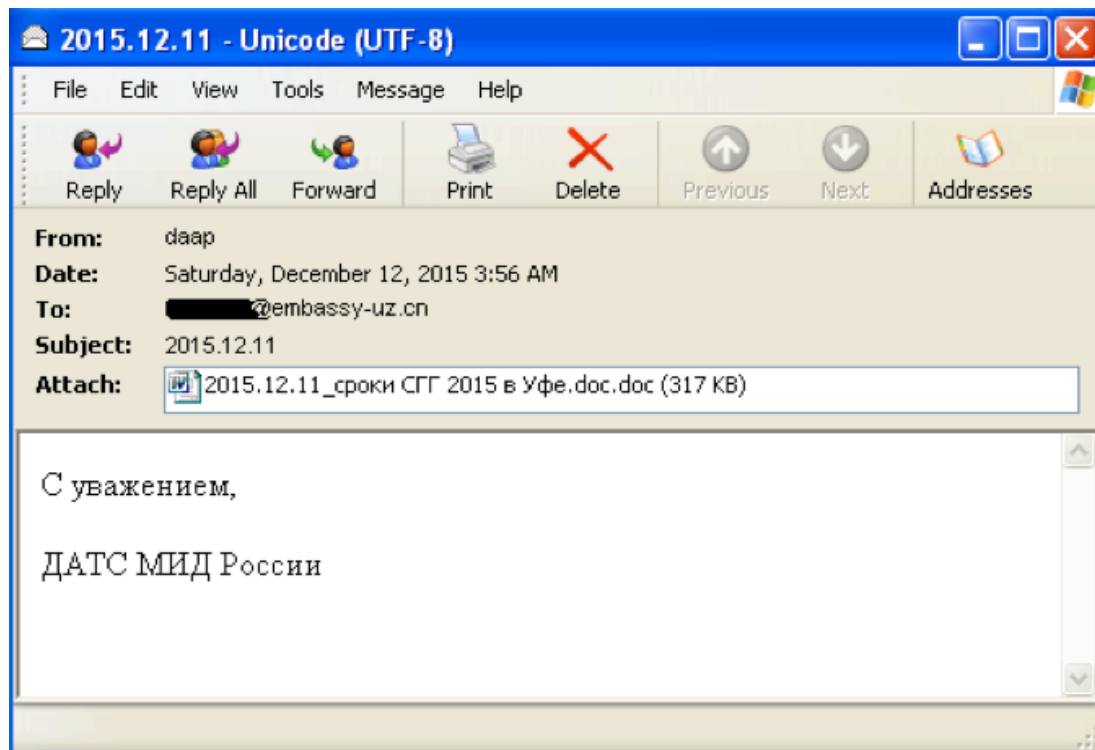
Command	Description
CAMERA	Take photos using system webcam and store them as c:\system\camera.jpg before sending to the C2.
AUDIO	Record audio from default audio input as c:\system\audio.ogg and sending it to the C2.
SCREEN	Take a screenshot and save it as c:\system\screenshot.bmp then send it to the C2.
KILL	Remove persistence registry entry and terminate itself.

POC on OpenCV library to capture video from webcam

#RSAC



NetTraveler TARGETS DIPLOMAT OF UZBEKISTAN

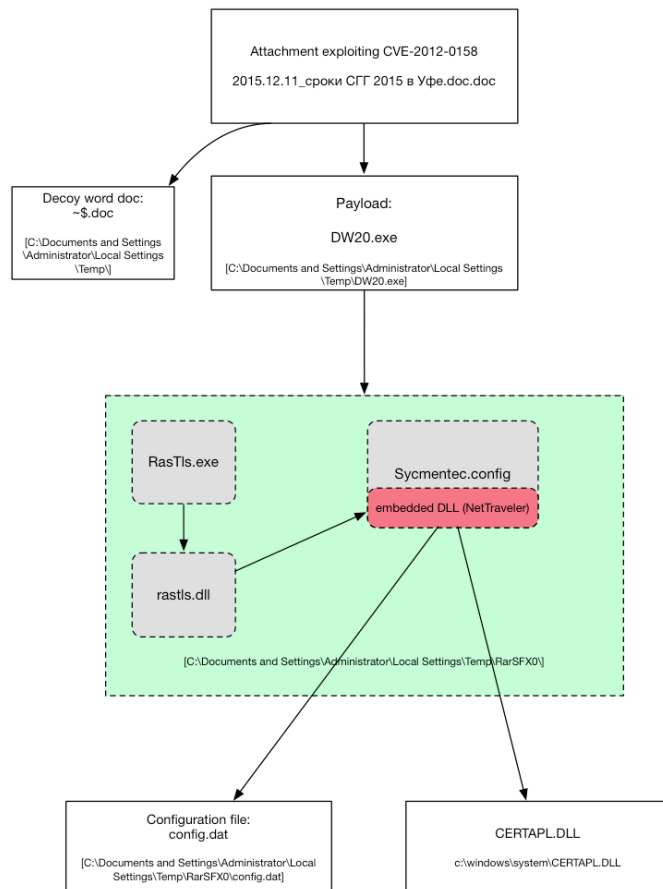


TARGETED SPEAR-PHISHING
EMAIL WAS SENT TO A
DIPLOMAT OF UZBEKISTAN

NetTraveler Targets diplomat of Uzbekistan



Infection Flow



DLL SIDE-LOADING
TECHNIQUE USED TO DROP
THE MAIN NETTRAVELER
PAYLOAD

NetTraveler configuration

```

mov     ecx, eax
push    offset aRastls_dll ; "\\rastls.dll"
push    esi
lea     eax, [ebp+Dest]
push    offset aSS         ; "ss"
push    eax                ; Dest
call    ebx ; sprintf
add     esp, 10h
lea     eax, [ebp+Dest]
push    edi                ; hTemplateFile
push    80h                ; dwFlagsAndAttributes
push    3                  ; dwCreationDisposition
push    edi                ; lpSecurityAttributes
push    1                  ; dwShareMode
push    80000000h          ; dwDesiredAccess
push    eax                ; lpFileName
call    ds:CreateFileA
cmp     eax, 0FFFFFFFFh
mov     [ebp+hObject], eax
jnz     short loc_100042D0

loc_100042D0:                ; dwMoveMethod
push    FILE_END
push    edi                ; lpDistanceToMoveHigh
push    -0B0h              ; lDistanceToMove
push    eax                ; hFile
call    ds:SetFilePointer
cmp     eax, 0FFFFFFFFh
jnz     short loc_100042F2

loc_100042F2:
lea     eax, [ebp+NumberOfBytesRead]
push    edi                ; lpOverlapped
push    eax                ; lpNumberOfBytesRead
push    0B0h              ; nNumberOfBytesToRead
push    offset aHttp192_168_3_201_downloader2013_asp ; "http://192.168.3.201/downloader2013/asp"
push    [ebp+hObject]      ; hFile
call    ds:ReadFile
test    eax, eax
js      short loc_100042E4

mov     dl, Default
push    40h
pop     ecx
xor     eax, eax
lea     edi, [ebp+var_11B]
mov     [ebp+FileName], dl
rep stosd
stosw
stosb
push    40h
xor     eax, eax
pop     ecx
lea     edi, [ebp+var_4A7]
mov     [ebp+filename_neverused], dl
push    esi
rep stosd
stosw
stosb
lea     eax, [ebp+FileName]
push    offset a_config_dat ; "ss\\config.dat"
push    eax                ; Dest
call    ebx ; sprintf

```

NetTraveler
obtaining its
configuration
from rastls.dll

NetTraveler DLL embedded in sycmentec.config

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	
00000930	ff	39	7a	77	9f	a0	81	88	88	f4	b3	7f	fc	22	7f	fe	y9zwY i "0* u"0b
00000940	35	57	1f	db	e5	43	77	1f	ff	39	7a	77	9f	c8	81	88	SW.04Cw.y9zwYBj ~
00000950	88	f4	b3	7f	fc	3a	7f	fe	36	6b	2a	b4	bb	bb	bb	bb	"0* u:0p6k* "www
00000960	22	fc	9b	cf	76	77	77	77	2a	b4	bb	bb	bb	bb	bb	bb	"u:Ivvvvv* "www
00000970	22	fc	9b	f4	9b	47	9f	42	77	77	77	fe	32	af	fa	32	"u>0YBwwwp2"u2
00000980	a7	27	9f	be	89	88	88	f4	b3	73	fa	3a	a7	26	9f	ba	S'YVa."0*su: S0Y*
00000990	88	88	88	f4	b3	73	f2	b7	03	7b	fa	22	a7	25	9f	fa	"0*so+. (u)"S0YU
000009a0	89	88	88	f4	b3	73	fc	92	2a	b4	bb	bb	bb	bb	bb	bb	u."0*su* "www
000009ba	9f	77	77	77	77	2f	f4	b7	72	b4	3a	2d	e7	77	74	77	Yvvvvv/0>0-0-gvzw
000009c0	77	77	73	77	77	77	88	88	77	77	cf	77	77	77	77	77	vvvvvvv"0Ivvvvvv
000009d0	77	77	37	77	77	77	77	77	77	77	77	77	77	77	77	77	vv7vvvvvvvvvvvvvvvv
000009e0	77	77	77	77	77	77	77	77	77	77	77	77	77	77	77	77	vvvvvvvvvvvvvvvvvv
000009f0	77	77	77	77	77	77	8f	77	77	77	79	68	cd	77	77	c3	vvvvvvvvvvvvvvvvvvvv
00000a00	7e	ba	56	cf	76	3b	ba	56	23	1f	1e	04	57	07	05	18	-0Viv:"V0...W...
00000a10	10	05	16	1a	57	14	16	19	19	18	03	57	15	12	57	05	...U...U...U...
00000a20	02	19	57	1e	19	57	33	38	24	57	1a	18	13	12	59	7a	..W...W384U...Yz
00000a30	7a	7d	53	77	77	77	77	77	77	77	3d	43	03	b4	79	22	z)3vvvvvvvvvvvvvvvv
00000a40	6d	e7	79	22	6d	e7	79	22	6d	e7	27	00	66	e7	7b	22	mqY"mqY"mq'.f0("
00000a50	6d	e7	02	3e	61	e7	7c	22	6d	e7	16	3d	66	e7	78	22	mq.>0q "mq.=f0x"
00000a60	6d	e7	fa	3e	63	e7	7d	22	6d	e7	16	3d	67	e7	7d	22	mq0>0q "mq.=0q "
00000a70	6d	e7	16	3d	69	e7	7d	22	6d	e7	79	22	6d	e7	78	22	mq.=10q "mqY"mq"
00000a80	6d	e7	ba	2d	32	e7	78	22	6d	e7	79	22	6c	e7	b9	22	mq"-20x"mqY"10"
00000a90	6d	e7	ba	2d	30	e7	6c	22	6d	e7	91	3d	66	e7	71	22	mq"-0q1"mq'=f0q"
00000aa0	6d	e7	25	1e	14	1f	79	22	6d	e7	77	77	77	77	77	77	mq....Y"mqvvvvvv
00000ab0	77	77	27	32	77	77	3b	76	72	77	70	5c	3c	21	77	77	vv'2vvv/vvzv < vv

26

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	
00000930	88	4e	0d	00	e8	d7	f6	ff	ff	83	c4	08	8b	55	08	89	"N..0-0yyFA..U..k
00000940	42	20	68	ac	92	34	00	68	88	4e	0d	00	e8	bf	f6	ff	B h-/4.h"m..e0y
00000950	ff	83	c4	08	8b	4d	08	89	41	1c	5d	c3	cc	cc	cc	cc	yyFA..M..A..jAIIII
00000960	55	8b	ec	b8	01	00	00	00	5d	c3	cc	cc	cc	cc	cc	cc	U0i.....jAIIIIII
00000970	55	8b	ec	83	ec	30	e8	35	00	00	00	89	45	d8	8d	45	U0i0i0e3...MEME
00000980	d0	50	e8	c9	fe	ff	ff	83	c4	04	8d	4d	d0	51	e8	cd	BTeEpyyFA..MDQ0I
00000990	ff	ff	ff	83	c4	04	85	c0	74	0c	8d	55	d0	52	e8	8d	pyyFA..At..f0Dhej
000009a0	fe	ff	ff	83	c4	04	8b	e5	5d	c3	cc	cc	cc	cc	cc	cc	pyyFA..0jAIIIIII
000009ba	e8	00	00	00	00	58	83	c0	05	c3	4d	5a	90	00	03	00	0....XFA..00...
000009c0	00	00	04	00	00	00	ff	ff	00	00	b8	00	00	00	00	00yy.....
000009d0	00	00	40	00	00	00	00	00	00	00	00	00	00	00	00	00	..0.....
000009e0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000009f0	00	00	00	00	00	00	f8	00	00	00	0e	1f	ba	0e	00	b40....."
00000a00	09	cd	21	b8	01	4c	cd	21	54	68	69	73	20	70	72	6f	..I'..li'This pro
00000a10	67	72	61	6d	20	63	61	6e	6e	6f	74	20	62	65	20	72	gram cannot be e
00000a20	75	6e	20	69	6e	20	44	4f	53	20	6d	6f	64	65	2e	0d	in in DOS mode..
00000a30	0d	0a	24	00	00	00	00	00	00	00	4a	34	74	c3	0e	55	..0.....04tA..
00000a40	1a	90	0e	55	1a	90	0e	55	1a	90	50	77	11	90	0c	55	..U..U..U..U..U..U
00000a50	1a	90	75	49	16	90	0b	55	1a	90	61	4a	11	90	0f	55	..U..U..U..U..U..U
00000a60	1a	90	8d	49	14	90	0a	55	1a	90	61	4a	10	90	0a	55	..U..U..U..U..U..U
00000a70	1a	90	61	4a	1e	90	0a	55	1a	90	0e	55	1a	90	0f	55	..U..U..U..U..U..U
00000a80	1a	90	cd	5a	45	90	0f	55	1a	90	0e	55	1b	90	ce	55	..U..U..U..U..U..U
00000a90	1a	90	cd	5a	47	90	1b	55	1a	90	e6	4a	11	90	06	55	..U..U..U..U..U..U
00000aa0	1a	90	52	69	63	68	0e	55	1a	90	00	00	00	00	00	00	..Rich..U..U.....
00000ab0	00	00	50	45	00	00	4c	01	05	00	07	2b	4b	56	00	00	..PE..U..U.....0YV..

C2 Infrastructure

No.	Source	Destination	Protocol	Length	Info
58	192.168.167.195	192.168.167.1	DNS	79	Standard query 0x0add A www.voennovosti.com
62	192.168.167.1	192.168.167.195	DNS	95	Standard query response 0x0add A 98.126.38.107

Queries

www.voennovosti.com: type A, class IN

Answers

www.voennovosti.com: type A, class IN, addr 98.126.38.107

Name: www.voennovosti.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 2 hours
Data length: 4
Addr: 98.126.38.107 (98.126.38.107)

0000	00 0c 29 bf 04 64 ac 9e 17 64 88 e7 08 00 45 00	..).d.. .d....E.
0010	00 51 00 00 40 00 40 11 6a 86 c0 a8 a7 01 c0 a8	.Q..@.@. j.....
0020	a7 c3 00 35 04 0e 00 3d 55 fa 0a dd 81 80 00 01	...5...= U.....
0030	00 01 00 00 00 00 03 77 77 77 0b 76 6f 65 6e 6ew ww.voenn
0040	6f 76 6f 73 74 69 03 63 6f 6d 00 00 01 00 01 c0	ovosti.c om.....
0050	0c 00 01 00 01 00 00 1c 20 00 04 62 7e 26 6bb~&k

C2 resolves to
'98.126.38[.]107' which
is hosted by Krypt
Technologies.

DLL side loading techniques continues to be used

● JP CERT report on attacks targeting Japan

Apr 03, 2017

RedLeaves - Malware Based on Open Source RAT

Hi again, this is Shusei Tomonaga from the Analysis Center.

Since around October 2016, JPCERT/CC has been confirming information leakage and other damages caused by malware 'RedLeaves'. It is a new type of malware which has been observed since 2016 in attachments to targeted emails.

This entry introduces details of RedLeaves and results of our analysis including its relation to PlugX, and a tool which is used as the base of this malware.

How RedLeaves runs

To have the RedLeaves injected into the process of Internet Explorer, the following steps will be taken (Figure1):

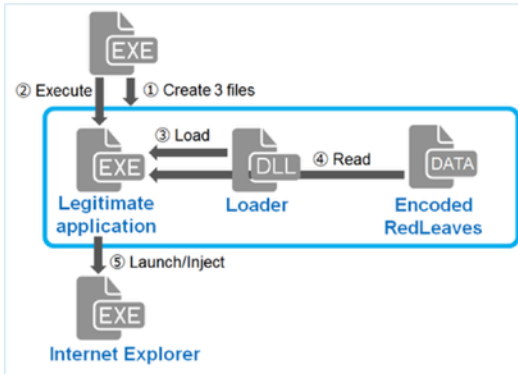


Figure 1: Flow of events until RedLeaves runs

● South Korean media reports on recent attacks

전체기사 | SECURITY | IT | DEFENSE | 시사리포트 | 로그인 | 회원가입 | 객원기자 | 기사제보 | 사이트맵

Home > 전체기사 > 사건·사고

[단독] 북한 해커조직, '사이버 논리폭탄' 탑재한 경찰용 악성코드 유포!

Like 181 | 입력: 2017-05-18 18:25 | 가 가

경찰 유지 위해 아래한글 프로그램에 가해지는 새로운 방식
오후 2시~6시 사이에만 특정 동작 수행하는 사이버 논리폭탄 탑재

[보안뉴스 권 준 기자] 북한 추정 해커조직이 최근 '사이버 논리폭탄'이 적용된 경찰용 악성 코드를 국내에 은밀히 유포하고 있는 것으로 드러났다.

Name	Description	Company Name	Version
HmcPmcCore9.dll			
HmcSDS.dll			
HmcSDS.kor			
HmcSpeller90.dll	Hancom Inc., HmcSpeller 9.0	Hancom Inc.	9.6.1.5040
HmcSpeller90.kor	Hancom Inc., HmcSpeller 9.0	Hancom Inc.	9.6.1.5040
HmcVfs90.dll	Hancom Inc., HmcVfs 9.0	Hancom Inc.	9.6.1.5040
HmcVfs90.kor	Hancom Inc., HmcVfs 9.0	Hancom Inc.	9.6.1.5040
HmcWebBrowser...	Hancom Inc., HmcWebBrowse...	Hancom Inc.	1.0.0.1
HmcWebDAV.dll	HmcVfsWe...		1.0.0.1
HmcWebDAV.kor	HmcVfsWe...		1.0.0.1
HmcXalCore9.dll	Dynamic Link Library for Xal...	Apache Software Fou...	1.10.0.0
HmcXalMsg9.dll	Dynamic Link Library for Xal...	Apache Software Fou...	1.10.0.0
HmcXalCore9.dll	Shared Library for Xarces-C...	Apache Software Fou...	2.7.0.0

▲ '아래한글' 프로그램에 가세하여 로드된 북한 경찰용 악성코드[자료=이슈메이커스랩]

사이버전 악성코드 전문 추적·연구 그룹 이슈메이커스랩의 '사이버전 연구센터'에 따르면 최

가장 많이 본 기사 >>

- 1 악영 달렸던 케르베르 랜섬웨어, 간판 바꿔 국...
- 2 아니니머스가 한국의 대학교 6곳을 해킹했다
- 3 군인 봉급 인상 공약으로 실패한 병장 월급 '...
- 4 윈도우 10 업데이트는 랜섬웨어 지옥에서 우리...
- 5 케르베르 이어 매트릭스 랜섬웨어도 귀환! 할 ...
- 6 [보안IT산업 동향] 한컴그룹, 개인안전장비...
- 7 사이버 공간에서도 출몰하는 테러리스트들, 해킹...
- 8 2017 정보보호의 날, 정보보호 유공자 14...
- 9 2017년 '보안의 혼란' 하루... 끊임 없는...
- 10 [주말면] 클라우드 고민하는 실무자들을 위한 ...

1분이면 OK
내 PC, 내 자료는 내가 지킨다
실시간악성코드 탐지 + 실시간악성코드 분석
BASIC SECURITY PLUS

(ISC)²
무료 최신 정보보안 온라인 세미나
2017년 5월 18일

ENDPOINT PROTECTION
(주)코스시스코리아
국내용 CC인증 획득
100% 국내생산 및 조달등록
해상도에 및 자료유출방지

What do we learn from the attacks?

- Threat actors continue to use old proven exploits – and it works.
- Threat actors employ new techniques to by-pass traditional security systems. We need to understand the TTPs to better defend against the threats.
- Asia Pacific continues to experience large number of growing targeted cyber attacks.
- Many threat actors continue to use same hosting providers for their C2 infrastructure

WAY FORWARD

- The risk from these attacks can be reduced significantly if systems are patched on a timely basis. PATCH PATCH PATCH!!!
- We need to understand the TTPs to better defend against the threats.
- Focus on “Preventing” a successful cyber attack.
- Education on the modus operandi of the threat actors.
- Unit 42 research includes TTPs and IOCs which is accessible to the public. Tools and resources also published in Github.

Questions ?

THANK YOU