Joint advisory by:

Military Counterintelligence Service
&
CERT.PL

SNOWYAMBER, HALFRIG, QUARTERRIG

IoC Reference

24 April 2023

v1.1

Table of Contents

Information

The purpose of this document is to provide a one-place IoC reference for any analyst that would like to recreate or validate SKW's & CERT.PL's findings. Provided IoCs should not be used as a reliable detection or defense mechanisms due to country-specific visibility and telemetry both teams have access to.

Both SKW and CERT.PL wish to provide broader cybersecurity community with means to analyze, track and hopefully disrupt adversary activity. Therefore all samples mentioned in SNOWYAMBER, HALFRIG and QUARTERRIG advisories shall be uploaded to VirusTotal, MalwareBaazar and MalShare services.

IoC reference sheet

SNOWYAMBER

Indicator	Value
Sample dated 24/10/2022	
File Name	7za.dll
File Size	270,336B
MD5	d0efe94196b4923eb644ec0b53d226cc
SHA1	c938934c0f53045410873133382aee163e0c5239c
SHA256	381a3c6c7e119f58dfde6f03a9890353a20badfa1bfa7c38ede62c6b0692103c

Indicator	Value
Sample dated 8/02/2023	
File Name	BugSplatRc64.dll
File Size	271,360B
MD5	cf36bf564fbb7d5ec4cec9b0f185f6c9
SHA1	8eb64670c10505322d45f6114bc9f7de0826e3a1
SHA256	e957326b2167fa7ccd508cbf531779a28bfce75eb2635ab81826a522979aeb98
Additional remarks	It seems that the adversary made a mistake while compiling this sample. Internal functions were added to exports (authored by the adversary as well as those from libraries: SysWhispers3, Nlohmann JSON, Obfuscate). While binary itself is stripped, those exported functions have names that can be demangled revealing naming, prototypes and datatypes.

Indicator	Value
Sample dated 7/02/2023	
File Name	BugSplatRc64.dll
File Size	301,056B
MD5	82ecb8474efe5fedcb8f57b8aafa93d2
SHA1	3fd43de3c9f7609c52da71c1fc4c01ce0b5ac74c
SHA256	4d92a4cecb62d237647a20d2cdfd944d5a29c1a14b274d729e9c8ccca1f0b68b

Indicator	Value
2nd stage - CobaltStrike beacon (decrypted)	
File Name	hXalk1725.pdf
File Size	261,635B
MD5	800db035f9b6f1e86a7f446a8a8e3947
SHA1	aaf973a56b17a0a82cf1b3a49ff68da1c50283d4
SHA256	032855b043108967a6c2de154624c16b70a0b7d0d0a0e93064b387f59537cc1e

Indicator	Value
2nd stage - BruteRatel stageless badger (decrypted)	
File Name	hXalk1314.pdf
File Size	347,837
MD5	0e594576bb36b025e80eab7c35dc885e
SHA1	a8a82a7da2979b128cbeddf4e70f9d5725ef666b
SHA256	ec687a447ca036b10c28c1f9e1e9cef9f2078fdbc2ffdb4d8dd32e834b310c0d

Value	Indicator	Role
totalmassasje.no/schedule.php	**URL**	ENVYSCOUT delivering SNOWYAMBER ZIP
signitivelogics.com/Schedule.html	**URL**	ENVYSCOUT delivering SNOWYAMBER ISO
humanecosmetics.com/category/noteworthy/6426-7346-9789	**URL**	Cobalt Strike Team Server
signitivelogics.com/BMW.html	**URL**	ENVYSCOUT delivering SNOWYAMBER ISO
badriatimimi.com	**Domain**	BRUTERATEL C2
literaturaelsalvador.com/Instructions.html	**URL**	ENVYSCOUT delivering SNOWYAMBER ZIP
literaturaelsalvador.com/Schedule.htm	**URL**	ENVYSCOUT delivering SNOWYAMBER ISO
parquesanrafael.cl/note.html	**URL**	ENVYSCOUT URL
inovaoftalmologia.com.br/form.html	**URL**	ENVYSCOUT URL

HALFRIG

Indicator	Value
Legitimate binary used for loading malicious DLL	
File Name	Note .exe
File Size	1597KB
MD5	83863beee3502e42ced7e4b6dacb9eac
SHA1	d9d40cb3e2fe05cf223dc0b592a592c132340042
SHA256	cb470d77087518ed7bc53ca624806c265ae2485d40ec212acc2559720940fb27

Indicator	Value
Virtual disc container	
File Name	Note.iso
File Size	2688KB
MD5	0e5ed33778ee9c020aa067546384abcb
SHA1	fbb482415f5312ed64b3a0ebee7fed5e6610c21a
SHA256	d1455c42553fab54e78c874525c812aaefb1f3cc69f9c314649bd6e4e57b9fa9

Indicator	Value
1st module	
File Name	AppvIsvSubsystems64.dll
File Size	27KB
MD5	f532c0247b683de8936982e86876093b
SHA1	f61e0d09be2fc81d6f325aa7041be6136a747c2d
SHA256	ddf218e4e7ccd5e8bd502fb115d1e7fbfaa393fb7e0b3b9001168caebc771c50

Indicator	Value
2nd module	
File Name	msword.dll
File Size	53KB
MD5	abc87df854f31725dd1d7231f6f07354
SHA1	e418d37fdcf4c288884bfe744b416cbdb0243a9e
SHA256	efeb7d9d0fabe464a32c4e33fe756d6ef7a9b369c0f1462b3dd573b6b667488e

Indicator	Value
3rd module	
File Name	envsrv.dll
File Size	56KB
MD5	2ffaa8cbc7f0d21d03d3dd897d974dba
SHA1	6dff9a9f13300a5ce72a70d907ff7854599e990a
SHA256	cfa65036aff012d7478694ea733e3e882cf8e18f336af5fba3ed2ef29160d45b

Indicator	Value
4th module (shellcode stager)	
File Name	mschost.dll
File Size	391KB
MD5	5b6d8a474c556fe327004ed8a33edcdb
SHA1	a677b6aa958fe02cac0730d36e8123648e02884f
SHA256	86edfd6c7a2fab8c50a372494e3d5b08c032cca754396f6e288d5d4c5738cb4c

Value	Indicator	Role
sawabfoundation.net/p.php?ip=<IP>&ua=<USER_AGENT>	**URL pattern**	ENVYSCOUT backend fingerprint collector
sawabfoundation.net/note.html	**URL**	ENVYSCOUT
sawabfoundation.net	**Domain**	compromised hosting used for ENVYSCOUT
communitypowersports.com	**Domain**	Actual CobaltStrike C2[1]
sanjosemotosport.com	**Domain**	CobaltStrike redirector

[1] We would like to express our thanks to multiple parties that reported the typo (erroneous labeling) in Network IoC section.

QUARTERRIG

Indicator	Value
Virtual disc container	
File Name	Note.iso
File Size	2624KB
MD5	22adbffd1dbf3e13d036f936049a2e98
SHA1	52932be0bd8e381127aab9c639e6699fd1ecf268
SHA256	c03292fca415b51d08da32e2f7226f66382eb391e19d53e3d81e3e3ba73aa8c1

Indicator	Value
Legitimate executable used to load the malicious DLL	
File Name	Note.exe
File Size	1600KB
MD5	b1820abc3a1ce2d32af04c18f9d2bfc3
SHA1	b260d80fa81885d63565773480ca1e436ab657a0
SHA256	6c55195f025fb895f9d0ec3edbf58bc0aa46c43eeb246cfb88eef1ae051171b3

Indicator	Value
QUARTERRIG - loader	
File Name	AppvIsvSubsystems64.dll
File Size	28KB
MD5	db2d9d2704d320ecbd606a8720c22559
SHA1	ca1ef3aeed9c0c5cfa355b6255a5ab238229a051
SHA256	18cc4c1577a5b3793ecc1e14db2883ffc6bf7c9792cf22d953c1482ffc124f5a

Indicator	Value
Encrypted resource containing the second stage	
File Name	bdcmetadataresource.xsd
File Size	456KB
MD5	166f7269c2a69d8d1294a753f9e53214
SHA1	02cd4148754c9337dfa2c3b0c31d9fdd064616a0
SHA256	3c4c2ade1d7a2c55d3df4c19de72a9a6f68d7a281f44a0336e55b6d0f54ec36a

Indicator	Value
Virtual disc container	
File Name	Invite.iso
File Size	6464KB
MD5	1609bcb75babd9a3e823811b4329b3b9
SHA1	86dcdf623d0951e2f804c9fb4ef816fa5e6a22c3
SHA256	91b42488d1b8e5b547b945714c76c2af16b9566b35757bf055cec1fee9dff1b0

Indicator	Value
Legitimate executable used to load the malicious DLL	
File Name	Invite.exe
File Size	5380KB
MD5	d2027751280330559d1b42867e063a0f
SHA1	15511f1944d96b6b51291e3a68a2a1a560d95305
SHA256	35271a5d3b8e046546417d174abd0839b9b5adfc6b89990fc67c852aafa9ebb0

Indicator	Value
QUATERRIG loader	
File Name	winhttp.dll
File Size	32KB
MD5	bd4cbcd9161e365067d0279b63a784ac
SHA1	b91e71d8867ed8bf33ec39d07f4f7fa2c1eeb386
SHA256	673f91a2085358e3266f466845366f30cf741060edeb31e9a93e2c92033bba28

Indicator	Value
Encrypted resource containing the second stage	
File Name	Stamp.aapp
File Size	460KB
MD5	8dcac7513d569ca41126987d876a9940
SHA1	1f65d068d0fbaec88e6bcce5f83771ab42a7a8c5
SHA256	9c6683fbb0bf44557472bcef94c213c25a56df539f46449a487a40eecb828a14

Indicator	Value
Virtual disc container	
File Name	Note.iso
File Size	2688KB
MD5	3aca0abdd7ec958a539705d5a4244196
SHA1	bacb46d2ce5dfcaf8544125903f69f01091bc3d6
SHA256	10f1c5462eb006246cb7af5d696163db5facc452befbfd525f72507bb925131d

Indicator	Value
QUATERRIG loader	
File Name	AppvIsvSubsystems64.dll
File Size	26KB
MD5	9159d3c58c5d970ed25c2db9c9487d7a
SHA1	6382ae2061c865ddcb9337f155ae2d036e232dfe
SHA256	a42dd6bea439b79db90067b84464e755488b784c3ee2e64ef169b9dcdd92b069

Indicator	Value
Encrypted resource containing the second stage	
File Name	bdcmetadataresource.xsd
File Size	479KB
MD5	bc4b0bd5da76b683cc28849b1eed504d
SHA1	b3ff6376baa180cff13ae76672c669cc8f45c130
SHA256	15d6036b6b8283571f947d325ea77364c9d48bfa064a865cd24678a466aa5e38

URL	Indicator	Role
pateke.com/auth/login.php	**URL**	QUARTERRIG C2 URL
pateke.com/index.php	**URL**	QUARTERRIG C2 URL
pateke.com	**Domain**	QUARTERRIG Domain
85.195.89.91	**IP address**	QUARTERRIG server IP
gatewan.com/c/msdownload/update/others/2021/10/se9fW4z8WJtmMyPQu	**URL**	COBALT STRIKE Handler URL
gatewan.com/c/msdownload/update/others/2021/10/8PaDBDxLtokI3eH8	**URL**	COBALT STRIKE Handler URL
gatewan.com	**Domain**	COBALT STRIKE C2 Domain
91.218.183.90	**IP address**	COBALT STRIKE C2 IP
sharpledge.com/login.php	**URL**	QUARTERRIG C2 URL
sharpledge.com	**Domain**	QUARTERRIG C2 Domain
51.75.210.218	**IP address**	QUARTERRIG server IP
sylvio.com.br/form.php	**URL**	URL to ENYVYSCOUT used to deliver QUARTERRIG
sylvio.com.br	**Domain**	Domain used to host ENVYSCOUT

CERT.PL

info@cert.pl

Military Counterintelligence Service

skw@skw.gov.pl