

样本分析报告

报告管理信息

报告版本	V1.0
文档创建者	陈之健
文档更新者	陈之健
文档创建时间	2021 年 8 月 23 日
文档修改时间	
样本发现时间	
保密级别	

样本信息

文件名	文件大小	文件 MD5
Maze	744448 bytes	27c5ecbb94b84c315d56673a851b6cf9

木马概述

此样本为 Maze（迷宫）勒索病毒，通过 shellcode 装载自身携带的 EXE 资源到自身进程内存空间，并跳转入口点执行，开始后续行为。被装载的 EXE 对自身文件进行了反反汇编处理，包括代码控制流平坦化、垃圾指令等手段。

木马勒索界面截图



木马特点：

木马执行细节

解密自身携带数据装载 PE，跳到装载后的入口点位置

004CE34E	FFB3 F8E34900	PUSH DWORD PTR DS:[EBX+0X49E3F8]	
004CE354	E8 B7230000	CALL 004D0710	
004CE359	895C24 10	MOV DWORD PTR SS:[ESP+0x10],EBX	
004CE35D	61	POPAD	
004CE35E	FFA3 C4E14900	JMP DWORD PTR DS:[EBX+0x49E1C4]	1.004219E0
004CE364	6A 00	PUSH 0x0	
004CE366	FF93 1CE84900	CALL DWORD PTR DS:[EBX+&&kerne132.ExitP	
004CE36C	C3	RET	
004CE36D	FF	PUSH EBP	

IsDebugPresent

在迷宫内检测[PEB+2]，如果被调试则进入死循环

RUN 跟踪，找迷宫出口

在本样本中的出口为 0x423815

反调试

InlineHook DbgUiRemoteBreakIn

地址	HEX 数据	反汇编	注释	寄存器 (MMX)
0043447D	8D4424 04	LEA EAX,DWORD PTR SS:[ESP+0x4]		EAX 0143FF20
00434481	C607 C3	MOV BYTE PTR DS:[EDI],0xC3		ECX 0143FEC4
00434484	50	PUSH EAX		EDX 771A70B4 ntdll.KiFastSystemCallRet
00434485	FF7A24 04	PUSH DWORD PTR SS:[ESP+0x4]		EBX 00000000
00434489	6A 01	PUSH 0x1		ESP 0143FF10 UNICODE ""
0043448B	57	PUSH EDI		EBP 0143FF94
0043448C	68 BD444300	PUSH 195ef8cf.004344BD		ESI 002A0000
00434491	0F84 4F660000	JE 195ef8cf.0043AAE6	JMP 到	EDI 771FF125 ntdll.DbgUiRemoteBreakin
00434497	75 0A	JNZ SHORT 195ef8cf.004344A3		EIP 00434481 195ef8cf.00434481
00434499	FF15 44C04300	CALL DWORD PTR DS:[0x43C044]	advapi	C 0 ES 0023 32 0 (FFFFFFFF)
0043449F	24 0A	AND AL,0xA		P 0 CS 001B 32 0 (FFFFFFFF)
004344A1	0000	ADD BYTE PTR DS:[EAX],AL		A 0 SS 0023 32 0 (FFFFFFFF)
004344A3	0F85 3D660000	JNZ 195ef8cf.0043AAE6	JMP 到	Z 0 DS 0023 32 0 (FFFFFFFF)
004344A9	74 0A	JE SHORT 195ef8cf.004344B5		

遍历进程，关闭进程

先将进程名进行简单加密，加密规则小写 Asc 码值减去 20 再与将差与差值右移 5 位值异或

135D5	0D5A 9F	LEA EBX,DWORD PTR DS:[EDX-0x61]	ECX 00000000
135D6	0D6A E0	LEA EBP,DWORD PTR DS:[EDX-0x20]	EDX 00000007
135D8	0F87D0	MOVZX EBX,DX	EBX 00000004
135DE	83FB 1A	CMP EBX,0x1A	ESP 0143FD2C UNICODE ""
135E1	0F43EA	CMOVB EBP,EDX	EBP 00000005
135EA	0F87D5	MOVZX EDX,0F	ESI 0143FD54 UNICODE "wininit.exe"
135E7	C1EA 05	SHR EDX,0x5	EDI 002A0000 UNICODE "UKLKLK0/GZG"
135EA	31EA	XOR EDX,EBP	EIP 004105F5 195ef8cf.004105F5
135EC	66:8914NF	MOV WORD PTR DS:[EDI+ECX*2],DX	C 0 ES 0023 32 0 (FFFFFFFF)
135F0	41	INC ECX	P 1 CS 001B 32 0 (FFFFFFFF)
135F1	39C8	CMP EAX,ECX	

查询相关资料，样本将加密后的进程名利用 Alder32 检验算法计算其校验值，初始值为(29a)

如果找到对应的就关闭进程

414122	68 32414100	PUSH 195ef8cf.00414133	EAX 757A2331 kernel32.TerminateProcess
414127	FFEB	JMP EAX	ECX 757A2331 kernel32.TerminateProcess
414129	FF15 F0C04300	CALL DWORD PTR DS:[0x43C0F0]	EDX 75814FC4 kernel32.75814FC4
41412F	71 0E	JNO SHORT 195ef8cf.0041413F	EBX 00000008
414131	0000	ADD BYTE PTR DS:[EAX],AL	ESP 0143FD20 ASCII "9AA"
414133	53	PUSH EBX	EBP 0143FD54 UNICODE "wininit.exe"
414134	68 66050000	PUSH 0x566	ESI 0143FD54 UNICODE "wininit.exe"

004136A0	83C4 0C	ADD ESP,0xC	
004136A3	3D 9205B055	CMP EAX,0x55B00592	
004136A8	0F8E 92000000	JLE 195ef8cf.00413740	
004136AE	3D EB057062	CMP EAX,0x627005EB	
004136B3	0F8E 17010000	JLE 195ef8cf.004137D0	
004136B9	3D 2F06E06D	CMP EAX,0x6DE0062F	
004136BE	0F8F 1B020000	JG 195ef8cf.004138DF	
004136C4	3D 0D06886B	CMP EAX,0x6888060D	
004136C9	89F5	MOV EBP,ESI	
004136CB	0F8E CA030000	JLE 195ef8cf.00413A9B	
004136D1	3D 2306106D	CMP EAX,0x6D100623	
004136D6	0F8F 5B070000	JG 195ef8cf.00413E37	
004136DC	3D 0E06886B	CMP EAX,0x6888060E	
004136E1	0F84 E9080000	JE 195ef8cf.00413FD0	
004136E7	75 04	JNZ SHORT 195ef8cf.004136ED	
004136E9	93	XCHG EAX,EBX	
004136EA	1000	ADC BYTE PTR DS:[EAX],AL	
004136EC	0075 0A	ADD BYTE PTR SS:[EBP+0xA],DH	
004136EF	74 04	JE SHORT 195ef8cf.004136F5	
004136F1	E9 200000EE	JMP EE413716	
004136F6	2100	AND DWORD PTR DS:[EAX],EAX	
004136F8	003D 14062E6C	ADD BYTE PTR DS:[0x6C2E0614],BH	
004136FE	0F84 CC080000	JE 195ef8cf.00413FD0	
00413704	75 04	JNZ SHORT 195ef8cf.0041370A	
00413706	890A	MOV DWORD PTR DS:[EDX],ECX	
00413708	0000	ADD BYTE PTR DS:[EAX],AL	
0041370A	75 25	JNZ SHORT 195ef8cf.00413731	
0041370C	74 04	JE SHORT 195ef8cf.00413712	
0041370E	77 22	JA SHORT 195ef8cf.00413732	
00413710	0000	ADD BYTE PTR DS:[EAX],AL	
00413712	68 2D374100	PUSH 195ef8cf.0041372D	
00413717	0F84 21730200	JE 195ef8cf.0043AA3E	JMP 到 kernel32.GetLastError

之后多次调用 IsDebuggerPresent，检测是否被调试。

获取用户信息

GetUserNameW 获取用户名

GetComputerNameW 获取计算机名

查询注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion 中的 ProductName 获取 Windows 产品名称

执行 WQL 搜索反病毒产品，wql select * from antivirusproduct 如果没有保存字符串"none|"

GetDriveTypeW,GetDiskFreeSpaceW 磁盘属性和空闲空间信息

GetVolumeInformationW 获取系统盘序列号信息

地区避免

GetUserDefaultUILanguage、GetSystemDefaultLangID 获取语言标识和下列标识 id 比较，如果相同释放保存信息的内存，退出当前线程

419: Russian

422: Ukrainian

423: Belarusian

428: Tajik

42B: hy-AM

42C: Azeri - Latin

437: Georgian

43F: Kazakh

440: Kyrgyz - Cyrillic

442: Turkmen

443: Uzbek - Latin
 444: Tarta
 818: Romanian - Moldova
 819: Russian - Moldova
 82C: Azeri - Cyrillic
 843: Uzbek - Cyrillic
 7C1A: Serbian
 6C1A: Serbian - Cyrillic
 1C1A: Serbian (Cyrillic, Bosnia and Herzegovina)
 281A: Serbian (Cyrillic, Serbia)
 81A: Serbian - Latin

地址	HEX 反汇编	汇编代码	注释
0043AA6E	FF25 E4C04300	JMP DWORD PTR DS:[0x43C0E4]	ntdll.RtlExitUserThread
0043AA76	CC9C 00430000	INT3	base129.ProcessThread

创建线程发送获取的数据

加密数据

83729304958372930dhejskrlt9483s

地址	HEX	反汇编	注释
024C0000	95 41 B2 2C DE 28 FD 54 77 14 14 B1 76 20 A1 EC	的??齋w■■貯 §	
024C0010	B8 D9 6F 0C BA 41 E1 E8 61 D1 AE 47 C0 FB 35 64	綱o.封徽a旬G利5d	
024C0020	D0 27 DC BA 69 A0 4F 9A 27 A6 6F EE 37 84 E8 92	?芎i煥? ?勳?	
024C0030	99 E6 EB FB 81 CF C7 77 2A 4A DF C7 CC 2F 68 6D	欄臟休恙*J味?hm	
024C0040	81 09 1F A0 F7 97 16 E3 13 5C 7D 36 77 DC CF 5B	?■鈴??\}6w三[
024C0050	C4 74 0B F6 7E 60 6F 4A 6D C8 B6 B8 8C 6B 27 C5	臙■鯨`oJm推竿k'?	
024C0060	55 B0 D8 CB E6 08 29 2A 9B 84 FC 89 F5 63 15 5C	U柏隨■)*証鼓鯪■\	
024C0070	87 42 AA E2 79 0E EF DE 59 6D E7 75 4D 89 8B ED	嗟 y■糖Ym錯M墜?	
024C0080	E4 4F 16 2E 46 6E 1E FC 75 AB FF 6C AB 7A 0D AB	鉦■.Fn■糖?1珙.?	
024C0090	9E 8F 78 83 5E 1B BD 0C 3A D5 B3 73 1F 83 4F 39	襖x偽■?:粘s■傲9	
024C00A0	ED 8D 10 C6 14 D6 CC 70 4C 68 30 C1 FF EF D7 36	韻■?痔pLh0?鑑6	
024C00B0	8C 4A 18 35 F0 A7 73 11 84 F7 34 B8 F2 AC 95 19	志■5販s■勾4蛤瑯■	
024C00C0	6F BC 51 D8 D5 16 24 D6 FC 1D 39 E6 5F 9A 8E 58	o檉占■\$貶■9鍬殞X	
024C00D0	2E 81 4D AD 88 02 76 F4 ED DC 6D 10 36 84 32 D4	.手璩U絲舫■6??	
024C00E0	DF 89 E7 7A 01 61 5A E0 77 17 C9 E8 1E BE 1C 35	邏鐸厶z鳥■设■?5	
024C00F0	48 EC 82 9F B5 92 15 37 55 F2 E7 17 DF F6 E9 E4	H朝燭?7U婢■若殇	
024C0100	0D 59 56 E4 5B B9 F7 8D FF 60 6E 2D 8D CF 2E C2	.YU鏹棍?`n-嶠.?	
024C0110	00 00 00 00 00 00 00 00 00 00 00 00 00 00	
024C0120	00 00 00 00 00 00 00 00 00 00 00 00 00 00	

发送前又加密了一次

合成 URL

URL 格式为 Http://IP/(dir+/{0,2})/[a-y]{1,10}suffix?{ [a-y]{1,4}=[a-z0-9]{1,10} }{0-4}

各个参数间用"&"隔开

1. IP 地址为以下 IP 中顺序挑选

91.218.114.4
 91.218.114.11
 91.218.114.25
 91.218.114.26
 91.218.114.31
 91.218.114.32

91.218.114.37

91.218.114.38

91.218.114.77

91.218.114.79

以 GetTickCount 的返回值作为随机数种子

随机数每次使用后更新

0423B98	8B4C24 04	MOV ECX,DWORD PTR SS:[ESP+0x4]	
0423B94	6901 FD430300	IMUL EAX,DWORD PTR DS:[ECX],0x343FD	
0423B9A	05 C39E2600	ADD EAX,0x269EC3	
0423B9F	8901	MOV DWORD PTR DS:[ECX],EAX	

2. dir 个数为(rand())&0x7fff)%3

每个通过 (rand())&0x7fff)%31 在下列字符串中选取

"news" "login" "register" "logout" "edit" "content" "private" "messages" "account" "view"
"webauth" "webaccess" "archive" "forum" "post" "signin" "signout" "update" "support" "ticket"
"task" "tracker" "analytics" "check" "checkout" "payout" "withdrawal" "sepa" "create" "transfer"
"wire"

3. 生成资源名 src 小写字母 a-y,字符个数为 1-10

4. 选取后缀名 suffix (rand())&0x7fff)%11

'.php','.asp','.aspx','.cgi','.jsp','.jspx','.do','.action','.html','.phtml','.shtml'

5. 参数的个数为((rand())&0x7fff)%5)

参数名字符长度为 1-4,字符为 a-y

参数值长度为 1-10,先判断随机数(rand())&0x7fff)是奇数还是偶数,如果是奇数,再次随机(rand())&0x7fff)%9 再加上 0x30,即为数字 0-8, 如果为偶数,则为字母[a-z]。

合成 Http 请求字符串,通过 send 发送给 IP 主机,之后再发送 Http 请求。

加密流程

1. 生成提示文件文本

CryptGenKey 和 CryptExportKey 导出 Rsa 密钥对,参数 0xA400 表示为 RSA 密钥交换算法

00403A0F	50	PUSH EAX	
00403AD0	68 01000000	PUSH 0x80000001	
00403AD5	68 00A40000	PUSH 0xA400	
00403ADA	FF7424 18	PUSH DWORD PTR SS:[ESP+0x18]	
00403ADE	68 213B4000	PUSH 195ef8cf.00403B21	
00403AE3	0F84 FF700300	JE 195ef8cf.00403BE8	JMP 到 advapi32.CryptGenKey
00403AE9	75 0A	JNZ SHORT 195ef8cf.00403AF5	
00403AEB	FF15 4CC04300	CALL DWORD PTR DS:[0x43C04C]	advapi32.EqualDomainSid

公钥导出 Blob

02460000	06 02 00 00	00 A4 00 00	52 53 41 31	00 08 00 00	■.?.RSA1.■..
02460010	01 00 01 00	61 C6 95 0A	28 78 D5 43	63 CA 96 8A	ㄟ.ㄟ.a莫.(x誅c藉?
02460020	2A BA 09 55	47 57 43 FE	34 C9 E8 11	B4 EF 34 DD	*?UGWC?没■达4?
02460030	61 CC 48 65	5B 88 26 FC	A0 10 61 E4	01 2A 40 33	a藁e[?藁■a?*03
02460040	B2 CB 08 8A	75 30 81 75	37 82 42 7C	57 B4 A0 23	菜■妖0壹7佟 W礮?
02460050	21 61 09 52	7D 72 12 2B	D5 5D C0 D7	1E A1 43 1E	?a.R>?r■+誠雷■
02460060	29 2C 05 3A	FA A2 5C 2F	37 95 E3 A9	36 C4 5B 6A),, ㄚ \7嚙?腫j
02460070	17 11 45 43	09 A5 E9 1B	AD 2E 6B FB	7D BE 79 CC	■■EC.ラ■?k嚙綯?
02460080	FE 41 B1 DA	57 48 6A A4	B6 CF 5B EE	66 46 E7 DA	設壁WHjさ蝶頭F纒
02460090	46 5B FA 94	94 3C 7E B4	18 DC E4 C5	C7 51 18 56	F[鷓?~?莪俳Q■U
024600A0	2C D4 8F 16	F7 82 47 97	DA 86 4A B0	5B 14 AF 25	,詮■配G複局癰?■?
024600B0	B7 6D 03 CE	3C FA 8A 72	A1 0E 1C CB	8A A2 CB 9E	機?鷓r?■富(?)?
024600C0	A8 ED 5F 2B	83 90 86 7B	63 16 94 AF	E1 7C 5F 62	+儼菴c■敵釀_t
024600D0	6F B1 34 2B	18 AD 40 30	AD C7 6D 1F	6A 62 67 BF	o?+■環0 m■jbg?
024600E0	EE 4F CD 07	BF 36 4D 6E	73 6B 82 0A	BC 19 A8 6C	類??Mnsk??-
024600F0	F9 0B E4 51	AF 05 9A 35	95 D6 1A DF	C2 41 92 77	?莖??嚙■呗A卅
02460100	DF 0A 44 C9	40 9D B4 4A	5A 74 9D BC	73 03 29 41	?D莖薄JZt;渾s)A
02460110	64 4E 79 89	00 00 00 00	00 00 00 00	00 00 00 00	dNy?.....
02460120	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02460130	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00

导入攻击者公钥

0A436C88	FF7424 18	PUSH DWORD PTR SS:[ESP+0x18]	
0A436C8C	FF76 04	PUSH DWORD PTR DS:[ESI+0x4]	
0A436C90	68 E56A3000	PUSH 195ef8cf.00A36CE5	
0A436C94	0F 8A 5E3F0000	JG 195ef8cf.00A36C18	JMP 到 advapi32.CryptImportKey
0A436C98	75 04	JNZ SHORT 195ef8cf.00A36CC0	
0A436CBC	F1	INT1	
0A436CBD	1F	POP DS	
0A436CBE	0000	ADD BYTE PTR DS:[EAX],AL	
0A436CC0	0F 85 523F0000	JNG 195ef8cf.00A36C18	JMP 到 advapi32.CryptImportKey
0A436CC4	7A 04	JB SHORT 195ef8cf.00A36CC0	
地址	HEX 数据	ASCII	
00050460	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0155E830 00A36CE5 19
00050470	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0155E834 002F5968
00050480	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0155E838 00050488
00050490	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0155E83C 00000114
000504A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0155E840 00000000
000504B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0155E844 00000000
000504C0	00 01 01 01 1A 01 00 00 00 02 00 00 00 A4 00 00	..#.#.■.?.	0155E848 02480000
000504D0	52 53 41 31 00 00 00 00 01 00 01 00 89 F2 3C FC	RSA1.■..去去詭<?	0155E84C 02480000
000504E0	08 88 E8 EB 6A 68 01 06 E7 35 27 20 C2 10 80 9A	指旋JK?? ?存	0155E850 00A4A0C0 19
000504F0	E3 D9 D6 00 FE C6 36 95 8A D6 56 CF 19 A8 8A 6F	亮? 6嚙詭■ o	0155E854 00050488
00050500	00 11 87 F3 CF 6A 1A 50 BF 99 94 50 1C C8 85 0D	■國端WP嚙指■注	0155E858 00000114
00050510	06 5E 66 DE FF 51 26 A0 51 A3 83 57 F2 A3 D4 88	讀F?Q&KQ W嚙嚙	0155E85C 00000000
00050520	3E 5F 07 AD 42 CB 87 F3 05 93 D0 56 AE 1A A8 A9	>■嚙嚙?嚙0?嚙	0155E860 00000000
00050530	3F 11 AF 4F 4F D4 34 7E E8 F7 AC EE F8 F9 9D 28	?■嚙0??性 ?	0155E864 00000000
00050540	50 DC C0 C3 F6 F5 38 7A D6 90 64 00 6A 13 23 FA	1帶岡?x嚙d]■?■	0155E868 00000000
00050550	82 43 2C 0F 0F A5 E3 12 9F 79 2B 61 70 F8 9C 68	嚙.o嚙?嚙+ap嚙k	0155E86C 00000000
00050560	02 60 50 EE C3 67 BE 6A CF 91 EE 05 49 16 C8 C0	嚙1嚙嚙嚙?1■入	0155E870 00000000
00050570	08 CF 0A 29 01 EF 1C 63 68 35 10 30 35 1F D8 19	嚙?x嚙嚙■-5?■	0155E874 00000000
00050580	51 80 AF E3 8A AD DA CA 70 15 80 08 68 38 A5 E8	0■ ■嚙嚙p■嚙h8■	0155E878 00000000
00050590	06 55 C2 78 E9 6A 7F 88 5C 58 01 80 25 85 22 6E	0U嚙嚙嚙■嚙x嚙?n	0155E87C 00000000
000505A0	32 82 ED BE 36 80 C0 7C F8 54 83 50 D5 86 84 E1	2嚙?嚙1嚙嚙嚙嚙	0155E880 00000000
000505B0	78 6F 6C 85 8F 3C 11 66 40 A9 CA 71 0C DC 08 44	x01嚙嚙<■F■ q.7D	0155E884 00000001
000505C0	00 A3 D0 AF BB 24 24 93 7D 11 10 3C 50 E7 18 46	.P \$\$\$嚙■CP?F	0155E888 02230000
000505D0	A8 97 9D 27 12 5A 5C 00 4C C0 05 80 00 00 00 00	?M2\■嚙嚙?...	0155E88C 00000001
000505E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0155E890 00000000

获取随机值 CryptGenRomdon,32 字节 key 和 8 字节 nonce，备份到内存的其他位置

0155ED5C	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155ED6C	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155ED7C	00 00 00 00	00 00 00 00	00 00 00 00	E2 54 9A A0	4A 91 DA 55
0155ED8C	74 C4 ED 3F	C9 EE 2B F2	D0 38 E3 65	64 AB 4C F9
0155ED9C	B6 92 0F EE	61 64 9E 96	00 00 00 00	00 00 00 00	00 00 00 00
0155EDA0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EDBC	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EDCC	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EDDC	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EDE0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EDFC	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EE00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EE10	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EE20	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EE30	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EE40	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EE50	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EE60	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EE70	00 00 00 00	00 00 00 00	F5 C6 E8 A4	9C 3C CC 84
0155EE80	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EE90	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EEA0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EEB0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EEC0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EED0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EEE0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EEF0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0155EEF8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00

使用非常规 chacha 加密算法加密私钥

在网上找了一篇描述 salsa 算法，与 chacha 算法类似

<https://www.cnblogs.com/initOne/p/14772868.html>

Expand 32-byte key 0 noncy 的初始矩阵，生成随机字节流 64 字节，每次处理 64 字节与原文异或生成密文，剩余的部分按字节异或，加密密钥共 0x494 字节。

CE 25 63 0C	A3 31 83 39	E2 99 F3 FD	C2 75 B1 10	?c.??鈹斷聯?
9E A7 FE 78	6F DB AB 90	ED 4F A3 47	D7 7A 96 FD	灑糴o鄧愴0 謔櫟
A4 89 55 B2	84 F5 F7 50	ED 4B 8F FB	BC E3 1A 96	U噪貅P鍵任爻■?
C2 24 E6 E8	76 55 9D 2F	47 A9 59 29	30 76 A5 EA	?骅uU?G ^{TEL})0uリ
A2 C4 2B 69	0B CE BA 02	16 4E 5E A9	97 66 06 BD	20.+i■魏■N^ f■?
A2 D7 91 22	53 7D 0B 07	7F 6D E7 28	D3 1C FE 4E	(9)?S}■■■m??銑
3C B9 F2 16	C0 FB 26 11	19 4C 19 B2	78 F2 C1 D8	<跪■利&■LL■瞞姑?
E5 1E F2 94	AE 7E 50 76	13 AD D7 B5	D7 A7 C8 82	?驍岫Pu■ 底 ?
FF A0 7A 27	E5 DD 94 96	75 57 67 89	B9 14 7B 26	讐龍'過救uWg█<&
34 DB 42 FA	8A 13 48 C3	79 63 D8 AC	0A B1 55 9B	4阻鷄■H胞c靈.盪?
CB DC D6 26	1B E2 80 9F	F5 52 70 DA	AF 37 FB 3C	塑?■欽敦Rp沼?
62 AC 27 0D	9F 38 6F C9	D1 09 BB 6B	A5 2F EB DD	b?.?o裳.簫?胼
B4 50 79 A9	D0 BB B7 3F	CD 56 6F 4B	DD A9 90 BA	碣y丁环?蛭ok季惡
D6 E7 05 0F	FD 99 35 FB	DD B1 57 BB	09 72 6E 49	昼■綠5 監?rnl
F0 D3 94 66	A7 DC 3C EE	58 01 1C 63	65 19 47 09	鸛撞K<頤■ce■G.
3C B4 F9 9A	1C BF 33 93	48 F5 9C 01	AF 1F 2A 87	<殆??摠養丹*?
2D 00 9F C7	11 4D 6A 49	55 8D 6E 8B	B4 15 84 19	-.煥■HjIU岢嫪■?
8E 98 B5 0E	5F EB 08 C3	E7 C5 CB 70	39 04 67 46	恰?_?苗潘p9 IgF
19 3E 20 D9	12 AA 94 F2	1E D4 A8 41	C0 A8 01 2B	■> ?矯?淵A括丑
38 55 3F BF	0B 43 C0 BD	11 8A 85 93	B8 44 D4 17	8U??C瀾■妳摳D?
C1 D2 10 53	A3 CE 3A 88	2E 76 66 1C	08 17 05 0C	烈■SN :?uf■■■丫
6D 61 51 F8	A4 CF 07 93	DE 12 54 D2	9D 22 71 11	maQ ?撚■T覷"q■
65 9A D3 82	26 C5 FA E2	8D 7D DC DB	7C 16 B4 A0	e釐?批釧}苗 ■襦
08 23 D4 DE	56 68 00 FB	A9 AA 7A 3C	8C 54 F2 76	■#贊Uh. 獄<香騰
99 82 3D E8	1D 14 64 60	48 32 5C 44	8F CF 84 BB	棟=?■d`H2\D傍券

加密备份到内存的 key 和 noncy

CryptEncrypt

创建文件 C: /ProgramData/data1.tmp,写入末尾为 0x66611166 的 109 字节数据

CryptBinaryToStringA Base64 加密私钥+公钥+加密后的 key 和 noncy, 加上字符串 NAOSEC, 通过函数 ZwSetEaFile 设置为文件扩展属性

地址	HEX 数据	ASCII
01CA0000	00 00 00 00 00 06 38 0A■8.NAOSEC.z
01CA0010	69 56 6A 44 4B 4D 78 67	iUjDKMxgznimfP9w
01CA0020	6E 57 78 45 4A 36 6E 2F	nWxEJ6n/nhv26uQ7
01CA0030	55 2B 6A 52 39 64 30 6C	U+jR9d6lv2kiUWyh
01CA0040	50 58 33 55 4F 31 4C 6A	PX3U01Lj/u84xqWw
01CA0050	69 54 6D 36 48 5A 56 6E	iTm6HZUnS9HqUkpM
01CA0060	48 61 6C 36 71 64 4C 45	Ha16qLEK2kLzroCF
01CA0070	6B 35 65 71 5A 64 6D 42	k5eqZdmBr2i15EiU
01CA0080	33 30 4C 42 33 39 74 35	30LB39t5yjTHP50P
01CA0090	4C 6E 79 46 73 44 37 4A	LnyFsD7JhE2TBmye
01CA00A0	50 4C 42 32 4F 55 65 38	PLB20Ue8pSuf1B2E
01CA00B0	36 33 58 74 64 65 6E 79	63Xtdeny1L/oHon5
01CA00C0	64 32 55 6C 6E 56 58 5A	d2U1nUX24m5FHsmN
01CA00D0	4E 74 43 2B 6F 6F 54 53	NtC+ooTSMN5Y9isC
01CA00E0	72 46 56 6D 38 76 63 31	rFUm8vc1iYb4oCF9
01CA00F0	56 4A 77 32 71 38 33 2B	UJw2q83+zxirCcNn

填充勒索提示文件中 Base64key 为 CryptBinaryToStringA Base64 私钥+获取的用户信息

2. 删除卷影副本

0155F178	7717E0ED	ntdll.7717E0ED
0155F17C	00389100	
0155F180	00415722	rCALL 到 CreateProcessV
0155F184	00000000	ModuleFileName = NULL
0155F188	028C0000	CommandLine = ""C:\pgdwy\orn\Fuck\...\Windows\dubbc\h\drd\...\system32\wkq\ienjv\peyt\...\uben\drge\tc\...\umic.exe" shadowcopy delete"
0155F18C	00000000	pProcessSecurity = NULL
0155F190	00000000	pThreadSecurity = NULL
0155F194	00000000	InheritHandles = FALSE
0155F198	00000000	CreationFlags = 0
0155F19C	00000000	pEnvironment = NULL
0155F1A0	00000000	CurrentDir = NULL
0155F1A4	0155F18C	pStartupInfo = 0155F18C
0155F1A8	0155F22C	pProcessInfo = 0155F22C
0155F1AC	00000000	

C: \Windows\system32\wmic.exe 执行 shadowcopy delete 删除卷影

3. 导入用户公钥

74b3510f 74b351e4 74b351e9 74b351f0 74b35224	68 28 68 4818d474 E8 57370000 33f6 8975 04 0000	PUSH 0x28 PUSH cryptsp.74b41848 CALL cryptsp.74b38940 XOR ESI,ESI MOV DWORD PTR SS:[EBP-0x2C],ESI XOR EBX,EBX	EAX 02250000 ECX 74b364c8 cryptsp.74b3 EDX 00000000 EBX 02680000 ESP 0294ff58 ASCII "表c" EBP 0294ff94 ESI 02250000 EDI 02680000
地址	HEX 数据	ASCII	
02670000	06 02 00 00 00 0A 00 00 52 53 41 31 00 08 00 00	0...?..RS01..	029AFF58 00A36CE5
02670001	01 00 01 00 61 C6 95 00 28 78 D5 43 69 CA 96 8A	...?..(???)	029AFF5C 002F5A78
02670002	2A BA 09 55 47 57 A3 FE 3A C9 E8 11 BA EF 3A DD	*TUGVC?..达A?	029AFF60 02670000
02670003	61 CC A8 05 5B 88 26 FC 00 10 61 E4 01 2A 40 33	...?..?..?..	029AFF64 00000114
02670004	02 08 0A 75 3B 81 75 37 82 A2 70 57 BA A8 23	...?..?..?..	029AFF68 00000000
02670005	21 61 09 52 70 72 12 2B 05 50 C0 D7 1E A1 43 1E	...?..?..?..	029AFF6C 00000000
02670006	29 2C 05 3A FA A2 5C 2F 37 95 E3 89 36 CA 58 6A	...?..?..?..	029AFF70 02250000
02670007	17 11 45 A3 09 A5 E9 18 A0 2E 68 F8 7D BE 79 CC	...?..?..?..	029AFF74 02250000
02670008	FE A1 B1 00 57 A8 6A 0A 06 CF 5B EE 66 A6 E7 DA	...?..?..?..	029AFF78 00A266A0 ASCII "h0k0"
02670009	A6 58 FA 9A 9A 3C 7E 8A 18 DC E4 C5 C7 51 18 56	...?..?..?..	029AFF7C 02670000
0267000A	2C D4 8F 16 F7 82 A7 97 DA 86 A8 00 5B 14 AF 25	...?..?..?..	029AFF80 00000114
0267000B	87 6D 03 CE 3C FA 8A 72 A1 0E 1C C8 8A A2 C0 9E	...?..?..?..	029AFF84 00000000
0267000C	08 ED 5F 20 83 9B 86 78 63 16 9A AF E1 7C 5F 62	...?..?..?..	029AFF88 00000000
0267000D	6F B1 34 2B 18 A0 A0 30 A0 C7 6D 1F 6A 62 67 BF	...?..?..?..	029AFF8C 757B3CA5 返回到 kernel32.757B3CA5
0267000E	EE AF CD 07 BF 36 A0 6E 73 68 82 0A BC 19 A8 6C	...?..?..?..	029AFF90 02680000
0267000F	19 00 E4 51 AF 05 9A 35 95 D6 1A DF C2 A1 92 77	...?..?..?..	029AFF94 029AFFD4
02670010	0F 0A C9 A8 9D 0A A6 5A 7A 9D 0C 73 03 29 A1	...?..?..?..	029AFF98 771C37F5 返回到 ntdll.771C37F5
02670011	64 AE 79 89 00 00 00 00 00 00 00 00 00 00 00	...?..?..?..	029AFF9C 02680000
02670012	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...?..?..?..	029AFFA0 75B77204 iertutil.75B77204
02670013	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...?..?..?..	029AFFA4 00000000

4. 遍历文件加密

68 B35A200 0F84 97500100 75 0A FF15 04C14300 2E:0000 0000 95A5 50010074 04 57 1E 0000 ED 1A 00 0083 F8FF0F84 C50400 003E 00	PUSH 0x4 PUSH 195ef8cf.00A25A83 JMP SHORT 195ef8cf.00A3A82E CALL DWORD PTR DS:[0x43C104] ADD BYTE PTR CS:[EAX],AL ADD BYTE PTR DS:[EDI],CL TEST DWORD PTR SS:[EBP+0x74000150],EAX ADD AL,0x57 PUSH DS ADD BYTE PTR DS:[EAX],AL IN EBX,DX ADC AL,0x0 ADD BYTE PTR DS:[EBX+0x8A00FFFF],AL LDS EAX,FWORD PTR DS:[EAX+EAX] ADD EBX,0x00000000	JMP 到 kernel32.FindFirstFileW kernel32.ExitProcess	ST1 empty 0.0 ST2 empty 0.0 ST3 empty 0.0 ST4 empty 0.0 ST5 empty 0.0 ST6 empty 0.0 ST7 empty 0.0 3 2 : FST 0000 Cond 0 0 1 FCW 027F Prec NEAR.
HEX 数据	ASCII		
43 00 3A 00 5C 00 2A 00 00 00 00 00 00 00 00	C.:.\.....	02C8F010 00025A83 195ef8cf.00A25A83	
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	02C8F000 025F0000 UNICODE "C:\""	
		02C8F004 02C8F014	

排除路径中含有以下字符串的文件，如果目录中不存在这些字符，则创建两个文件

DECRYPT-FILES.txt 勒索提示文件，{UID}.tmp 文件为空

\Program Files

:\Windows

\Games\

\Tor Browser\

\ProgramData\

\cache2\entries\

\Low\Content.IE5\

\User Data\Default\Cache\

\All Users

\IETIdCache\

\Local Settings\

\AppData\Local

AhnLab

{0AFACED1 - E828 - 11D1 - 9187- B532F1E9575D}

排除文件名位以下的文件

DECRYPT-FILES.txt

autorun.inf

boot.ini

desktop.ini

ntuser.dat

iconcache.db

bootsect.bak

ntuser.dat.log

thumbs.db

Bootfont.bin

排除以下后缀名文件

lnk.exe.sys.dll

SetFileAttributeW测试文件是否存在

使用CreateFileW打开文件，获取文件的大小，判断是否小于等于0x50000,再次判断文件大小是否大于108个字节时，再判断文件末尾4个字节是否是0x66611166

06 00	IMUL EAX,DWORD PTR DS:[ESI],0x0
3C12	ADD BYTE PTR DS:[EDX+EDX],BH
00	ADD BYTE PTR DS:[EAX],AL
0B	MOV ECX,DWORD PTR DS:[EBX]
9 00010000	CMP ECX,0x100
20	JB SHORT 195ef8cf.0042BF22
7C08 FC 6611	CMP DWORD PTR DS:[EAX+ECX*0x4],0x66611166
34 47030000	JE 195ef8cf.0042C257
04	JNZ SHORT 195ef8cf.0042BF16
00	INC EAX
00	ADD AL,0x0

判断条件成功后，开始加密

1. 获取随机的32字节的key和8字节的nonce

CryptGenRandom

地址	HEX 数据	ASCII
360000	78 A8 F2 42 36 E0 E7 BD 9E 30 A9 22 2D 2F AB 9E	x B6噠縊0?-/理
360010	A7 7D 86 EA 8C 44 3D DA E6 1E 0C 9E F0 F2 F2 60	噠縊=阪.负蚪
360020	2A 1A 75 1F 28 76 1D 4C 00 00 00 00 00 00 00 00	*u(UL.....
360030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
360040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

2. 备份key和noncy，然后RSA加密这两个值 CryptEncryptr 末尾增加感染标记
3. 使用chacha加密
4. 将108字节的数据，被加密的key值和nonce值写到文件末尾

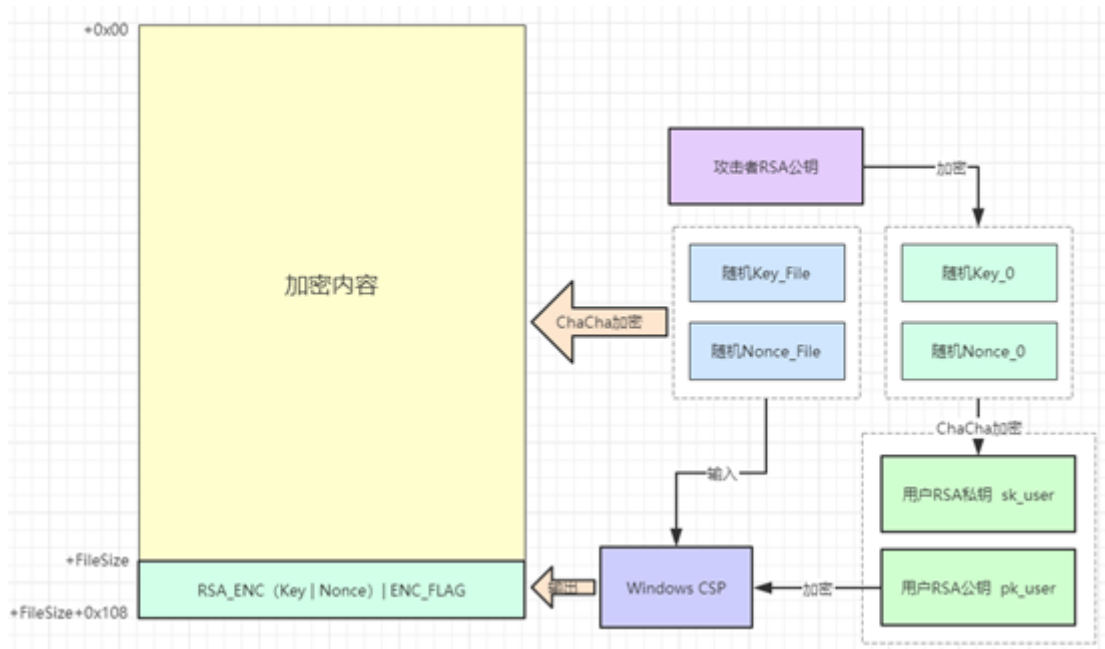
0042C100	68 1024200	PUSH 195ef8cf.0042C211		ESI 0042C100
0042C104	0F 55 25100000	JMP 195ef8cf.0042C100	JMP 到 kernel32.WriteFile	EIP 0042C101 195ef8cf.0042C101
0042C107	75 04	JNZ SHORT 195ef8cf.0042C1D0		C 0 ES 0020 32 0 (FFFFFFFF)
0042C109	DAB7	FIADD DWORD PTR DS:[EDI]		P 0 CS 0010 32 0 (FFFFFFFF)
0042C10B	0000	ADD BYTE PTR DS:[EAX],AL		A 0 SS 0020 32 0 (FFFFFFFF)
0042C10D	0F 85 19E80000	JNZ 195ef8cf.0042C0FC	JMP 到 kernel32.WriteFile	Z 0 DS 0020 32 0 (FFFFFFFF)
0042C10E	74 04	JE SHORT 195ef8cf.0042C1E9		S 0 FS 0000 32 0 7FFD0000(FFF)
0042C10F	0000	OR BYTE PTR DS:[EDI],CL		T 0 CS 0000 NULL
0042C110	0000	ADD BYTE PTR DS:[EAX],AL		D 0
0042C111	0000	PUSH CS		D 0 LastErr ERROR_SUCCESS (00)
0042C112	1000	SBB EAX,DWORD PTR DS:[EAX]		EFL 00000202 (NO,NB,NE,A,NS,PO
0042C113	00C2	ADD DL,AH		M10 0000 0000 0000 0000
0042C114	1000	SBB AL,BYTE PTR DS:[EAX]		M11 0000 0000 0000 0000
0042C115	0000	ADD BYTE PTR DS:[EAX],DL		M12 0000 0000 0000 0000
0042C116	0000	SBB EAX,DWORD PTR DS:[EAX]		M13 0000 0000 0000 0000
0042C117	0000	ADD BYTE PTR DS:[ESI+0x5D000000],BL		M14 0000 0000 0000 0000
0042C118	1C 00	SBB AL,0x0		M15 0000 0000 0000 0000
0042C119	0000	ADD BYTE PTR DS:[EAX],CL		M16 0000 0000 0000 0000
0042C11A	1200	ADC AL,BYTE PTR DS:[EAX]		M17 0000 0000 0000 0000
0042C11B	0000 09	ADD BYTE PTR DS:[EAX+0x9],CH		
0042C11C	0000	ADD BYTE PTR DS:[EAX],AL		
0042C11D	00 1C	MOV AL,0x1C		
0042C11E	0000	ADD BYTE PTR DS:[EAX],AL		
0042C11F	0C 1C	CMPL AL,0xC		
0042C120	0000	ADD BYTE PTR DS:[EAX],AL		
0042C121	0000	ADD BYTE PTR DS:[ESI+0x11],0x0		

地址	HEX 数据	ASCII
02080000	EC 01 AC 68 0A 01 93 58 F8 9B 55 8D DE 2F A4	02080000 0042C211 195ef8cf.0042C211
02080010	D9 03 3E A2 48 09 21 C8 CA 9A 9A 54 76 1F 26 83	02080010 00000024
02080020	21 81 FB 98 FE 25 DC A6 87 0E 16 69 9C 5C 82	02080020 00000100
02080030	3B 68 FD 03 03 15 00 02 3B A6 92 66 A5 6A 02	02080030 00000000
02080040	09 A8 9A 0A 00 E1 68 FA A8 9B 93 C0 2A 85 C5 3A	02080040 00000000
02080050	0A 69 98 0D A1 A5 7B 6A AE 9C FA DC 6E 57 DE 17	02080050 00000000
02080060	E1 2A 03 4F AF 3F AF 71 0A AE 51 8C A8 AC 21 07	02080060 00000000
02080070	82 2B 02 00 9C E7 C8 3A E8 6A CD C3 A7 86 7A 00	02080070 00000000
02080080	F6 2A 1C 0B 06 3E 97 11 00 52 09 A3 D5 87 EA 69	02080080 00000000
02080090	0E E5 D7 E8 BA 67 F6 D0 2A C1 A1 05 8C DB C4 E8	02080090 00000000
020800A0	9A 17 19 EB A6 9C 29 AF E2 DB 05 0F 64 11 6F E0	020800A0 00000000
020800B0	7D 87 2A 0C 51 F9 0D F8 A6 82 75 30 F2 7C 07 00	020800B0 00000000
020800C0	7A 05 0A 73 85 0A 9A 62 9D 7A AE 3D 31 AB 22 00	020800C0 00000000
020800D0	31 8A 69 7A 2B 5E 35 31 E1 00 EF 8B 57 85 6A 3E	020800D0 00000000
020800E0	95 6E 9B 92 8A 8A 89 A6 DB 16 A7 E8 9C 10 87	020800E0 00000000
020800F0	9C 02 C9 09 1B 66 A7 73 AC AC C6 23 88 EC BF 06	020800F0 00000000
02080100	00 00 00 00 66 11 61 66 00 00 00 00 00 00 00	02080100 00000000

5. 生成随机的文件后缀名，随机方式类似URL字符串随机生成方式，字符组成为大小写字母和0-9数字

00430B20	- FF25 60C14300	JMP DWORD PTR DS:[0x43C160]	kernel32.HoveFileExW	EAX 00000010	
00430B2E	- FF25 60C14300	JMP DWORD PTR DS:[0x43C164]	kernel32.FindFirstFileW	ECX 780750AE	
00430B3A	- FF25 68C14300	JMP DWORD PTR DS:[0x43C168]	kernel32.WaitForMultipleObjects	EDX 00000000	
00430B3D	- FF25 60C14300	JMP DWORD PTR DS:[0x43C16C]	kernel32.GetDriveTypeW	EDX 02C8F268 UNICODE "C:\A\1.txt"	
00430B4B	- FF25 70C14300	JMP DWORD PTR DS:[0x43C170]	kernel32.GetTickCount64	ESP 02C8EAC	
00430B46	- FF25 60C14300	JMP DWORD PTR DS:[0x43C16C]	kernel32.SetThreadExecutionState	EBP 00000001	
00430B4C	- FF25 78C14300	JMP DWORD PTR DS:[0x43C178]	kernel32.GetCommandLineW	ESI 02C8EAC0 UNICODE "C:\A\1.txt.kh	
00430B52	- FF25 70C14300	JMP DWORD PTR DS:[0x43C17C]	kernel32.GetFileSizeEx	EDI 02C8E000	
DS:[0043C160]-7570A091 (kernel32.HoveFileExW)				EIP 00430B20 JMP 00430B20 kernel32.HoveFi	
地址	HEX 数据	ASCII	02C8EAC	00425820	
02C8E60	43 00 3A 00	5C 00 41 00	5C 00 31 00	2E 00 7A 00	C:\A\1.txt
02C8E70	78 00 74 00	2E 00 60 00	AE 00 46 00	6C 00 AE 00	x.t...k.N.J.I.N.
02C8E80	00 00 20 00	6C 4D 0A 75	00 00 20 00	50 01 20 00	...3Kcu...P...
02C8E90	00 00 00 00	00 00 00 00	50 01 20 00	02 00 00 02P.....
02C8E98	00 00 00 00	4F 00 00 4F	45 00 00 00	00 00 00 00OE.....
02C8E9B	00 00 00 00	03 00 00 00	00 00 00 00	45 00 00 00E.....
02C8EA0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EA4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EA8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EAC	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EAD	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EAE	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EAF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EB0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EB4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EB8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EBC	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EBF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EC0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EC4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EC8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8ECB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8ECF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8ED0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8ED4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8ED8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EDB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EDF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EE0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EE4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EE8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EEB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EEF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EF0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EF4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EF8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EFB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8EFF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F04	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F08	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F0B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F0F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F10	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F14	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F18	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F1B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F1F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F20	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F24	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F28	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F2B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F2F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F30	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F34	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F38	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F3B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F3F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F40	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F44	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F48	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F4B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F4F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F50	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F54	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F58	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F5B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F5F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F60	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F64	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F68	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F6B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F6F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F70	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F74	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F78	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F7B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F7F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F80	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F84	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F88	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F8B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F8F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F90	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F94	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F98	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F9B	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8F9F	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FA0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FA4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FA8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FAB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FAF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FB0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FB4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FB8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FBB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FBF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FC0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FC4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FC8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FCB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FCF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FD0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FD4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FD8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FDB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FDF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FE0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FE4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FE8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FEB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FEF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FF0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FF4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FF8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FFB	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02C8FFF	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00

加密流程图请参考文章中的图



IOCs

91.218.114.4
 91.218.114.11
 91.218.114.25
 91.218.114.26
 91.218.114.31
 91.218.114.32
 91.218.114.37
 91.218.114.38
 91.218.114.77
 91.218.114.79
 合成的 URL

参考文章

<https://bbs.360.cn/thread-15826039-1-1.html>