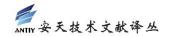


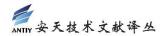
# Regin 模块 50251 和 Qwerty 击键记录器之对比

#### 非官方中文译文•安天技术公益翻译组 译注

文 档 信 息					
原文名称	Comparing the Regin module 50251 and the				
	"Qwerty" keylogger				
原文作者	Costin Raiu, Igor	原文发布	2015年1月27日		
	Soumenkov	日期			
作者简介	Costin Raiu 是卡巴斯基实验室全球研究和分析团队				
	的总监。也是一位自由思想家、软件开发员、建筑师、				
	摄影师、编辑。				
	http://securelist.com/author/costin/				
原文发布	卡巴斯基实验室				
单 位					
原文出处	http://securelist.com/blog/research/68525/comp				
	aring-the-regin-module-50251-and-the-Qwerty-				
	keylogger/				
译者	安天技术公益翻译组	校 对 者	安天技术公益翻译组		
免责声明	本译文译者为安天实验室工程师,本文系出自个人兴趣在业余时间所译,				
	本文原文来自互联网的公共方式,译者力图忠于所获得之电子版本进行翻				
	译,但受翻译水平和技术水平所限,不能完全保证译文完全与原文含义一				
	致,同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行				
	可靠性验证和评价。				
	本译文对应原文所有观点亦不	不受本译文中任	何打字、排版、印刷或翻译错		
	误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实				
	性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天				
	实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代				
	表译者和安天实验室对原文立场持有任何立场和态度。				
	译者与安天实验室均与原作者与原始发布者没有联系,亦未获得相关的版				
	权授权,鉴于译者及安天实验室出于学习参考之目的翻译本文,而无出版、				
	发售译文等任何商业利益意	图,因此亦不对	任何可能因此导致的版权问题		
	承担责任。				
	本文为安天内部参考文献,主要用于安天实验室内部进行外语和技术学习				
	使用,亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊				
	重译者的劳动和意愿,不得以任何方式修改本译文。译者和安天实验室并				
	未授权任何人士和第三方二次	欠分享本译文 ,	因此第三方对本译文的全部或		



者部分所做的分享、传播、报道、张贴行为,及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的,基于上述问题产生的法律责任,译者与安天实验室一律不予承担。



# Regin 模块 50251 和 Qwerty 击键记录器之对比

Costin Raiu, Igor Soumenko

2015年1月27日

2015年1月17日,《明镜周刊》发布了一篇根据爱德华·斯诺登提供的文件所编写的详细的文章。与此同时,他们提供了代号为"QWERTY"的恶意程序的副本,据说好几个政府在其CNE(计算机网络开发)活动中都用了这一程序

(http://www.spiegel.de/media/media-35668.pdf),

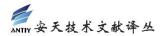
我们已经从《明镜周刊》获得了恶意文件的副本,当分析它们时,我们立刻联想到了 Regin。我们仔细地分析了代码,得出的结论是:Qwerty 恶意软件的功能与 Regin 50251 插件是完全一样的。

#### 分析

Qwerty 模块由 3 个二进制文件和相应的配置文件组成。其中的一个文件 20123.sys 尤其有趣。

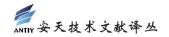
20123.sys 是 Qwerty 击键记录器的内核模式的一部分。事实证明,其源代码也存在于 Regin 的一个插件 50251 中。

使用二元差异法,可以很容易地发现两个文件所共享的大部分代码。



614	1889			
614	e0 74 18 80 7d e7 01 75	09 ff 75 e0 ff 15 f4 02	01 00 ff 75 e0 ff 15	.t2uu
62B 642	f8 02 01 00 33 c0 e8 13 6a 01 68 01 00 00 7f ff	98 99 99 c2 19 99 cc 53 35 98 15 91 99 32 db e8	68 c0 14 01 00 6a 0d f0 0b 00 00 85 c0 75	3 Sh i j.h52
659	02 fe c3 8a c3 5b c3 5c	00 44 00 65 00 76 00 69	00 63 00 65 00 5c 00	[.\.D.e.v.i.c.e.\
670	4b 00 65 00 79 00 62 00	6f 00 61 00 72 00 64 00	43 00 6c 00 61 00 73	K.e.y.b.o.a.r.d.C.1.a.s
687	00 73 00 30 00 00 00 00	00 6b 00 62 00 64 00 63	00 6c 00 61 00 73 00	.s.0k.b.d.c.l.a.s
69E	73 00 2e 00 73 00 79 00	73 00 00 00 55 8b ec 83	ec 14 53 68 60 06 01	ss.y.sUSh`.
6B5	00 8d 45 ec 50 32 db ff	15 b8 02 01 00 8d 45 f8	50 8d 45 f4 50 68 00	E.P2E.P.E.Ph
6CC	00 10 00 8d 45 ec 50 ff	15 c4 02 01 00 85 c0 0f	85 a0 01 00 00 39 45	E.P <u></u> 9E
6E3	f4 0f 84 a4 01 00 00 39	45 f8 0f 84 8e 01 00 00	ff 75 f4 e8 33 08 00	<u>.</u> 9Eu3
6FA 711	00 85 c0 89 45 f8 0f 84 8d 55 fc 52 50 ff 51 2c	7b 01 00 00 a1 08 15 01 84 c0 59 59 0f 84 5e 01	00 8b 48 04 8b 49 0c 00 00 8b 45 fc 8b 55	E(HI .U.RP.Q,YY^EU
728	f8 8b 52 08 8b 48 04 ff	72 44 8b 49 04 8b 49 0c	50 ff 91 38 01 00 00	RHrD.II.P8
73F	84 c0 59 59 0f 84 24 01	00 00 8b 55 f8 8b 45 fc	8b 52 08 8b 48 04 8b	YY\$UERH.
756	49 04 8b 49 0c 83 c2 44	52 50 ff 91 38 01 00 00	84 c0 59 59 0f 84 fd	IIDRP8YY
76D	00 00 00 8b 45 fc 8b 48	04 8b 49 04 8b 49 0c 68	5a 05 01 00 50 ff 91	EHII.hZP.
784	38 01 00 00 84 c0 59 59	0f 84 db 00 00 00 8b 45	fc 8b 48 04 8b 49 04	8YYEHI
79B	8b 49 0c 68 01 00 08 00	50 ff 91 2c 01 00 00 84	c0 59 59 0f 84 b9 00	.I. <u>h</u> P <sub>.</sub> <sub>.</sub> YY
7B2 7C9	00 00 8b 45 fc 8b 48 04 84 c0 59 59 0f 84 9a 00	8b 49 04 8b 49 0c 6a 00 00 00 8b 45 fc 8b 48 04	50 ff 91 2c 01 00 00 8b 49 04 8b 49 0c 6a	EHII.j.P, YYEHII.
7E0	02 50 ff 91 24 01 00 00	84 c0 59 59 74 7f 8b 45	fc 8b 48 04 8b 49 04	.P\$YYtEHI
7F7	8b 49 0c 6a 01 50 ff 91	24 01 00 00 84 00 59 59	74 64 8b 45 fc 8b 48	.I.j.P\$YYtd.E
80E	04 8b 49 04 8b 49 0c 68	90 06 01 00 50 ff 91 20	01 00 00 84 c0 59 59	II.hPY
825	74 46 8b 45 fc 8b 48 04	8b 49 04 8b 49 0c 6a 07	68 31 c4 00 00 68 01	tF.EHII.j.h1h
830	00 00 7f 50 ff 91 e0 00	00 00 83 c4 10 85 c0 75	20 8b 45 fc 8b 48 04	Pu .EH
853 86A	8b 49 04 8b 49 0c 68 00 02 fe c3 8b 45 fc 8b 40	15 01 00 50 ff 91 bc 01 04 8b 40 04 8b 40 0c 8d	00 00 84 c0 59 59 74 4d fc 51 ff 50 34 59	.II.hPYY: E@@@M.Q.P4
881	8b 4d f4 85 c9 74 06 ff	15 d0 02 01 00 8a c3 5b	c9 c3 cc 55 8b ec 83	.Mt
898	ec 0c 53 8d 45 f4 50 8d	45 f8 50 6a 01 68 01 00	00 7f ff 35 08 15 01	S.E.P.E.Pj.h5
8AF	00 c6 45 ff 00 32 db e8	39 0a 00 00 85 c0 75 28	83 7d f8 0d 75 12 56	E29u(,}ú.\
806	00 70 14 07 D1 C0	1122 / 11	ave styll)	O.W
8DD 8F4	50 e8 01 0b 00 00 20 00 c7 05 c9 14 01	)123 ("	gwerty")	Pu'.%
Olim	00 07 03 03 14 01	•		concorrect contract,
702	1803			
702	5d e0 74 18 80 7d e7 01	75 09 ff 75 e0 ff 15 d0	02 01 00 ff 75 e0 ff	1, t., 2, . u., u.,
702 719	5d e0 74 18 80 7d e7 01 15 d8 02 01 00 33 c0 e8	54 08 00 00 c2 10 00 53	68 60 13 <b>01 00 6a 0</b> 5	3TSh`i.
702 719 730	5d e0 74 18 80 7d e7 01 15 d8 02 01 00 33 c0 e8 6a 01 68 01 00 00 7T TT	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 qp e8	68 60 13 <b>01 00 6a</b> 05 6a 0a 00 00 85 c0 75	3TSh`i. j.n52ju
702 719	5d e0 74 18 80 7d e7 01 15 d8 02 01 00 33 c0 e8	54 08 00 00 c2 10 00 53	68 60 13 <b>01 00 6a 0</b> 5	3TSh`i.
702 719 730 747 75E 775	5d e8 74 18 88 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 68 01 00 00 7f ff 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 30 00 00 00 00	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63	68 60 13 01 00 6a 05 6a 0a 00 00 85 00 75 00 63 00 65 00 5c 00 43 00 6c 00 61 00 73 00 6c 00 61 00 73 00	3. TSh`i. j.ns2. jt[.\.D.e.v.i.c.e.\. K.e.y.b.o.a.r.d.C.1.a.s .s.0k.b.d.c.1.a.s
702 719 730 747 75E 775 78C	5d e0 74 18 80 7d e7 01 15 d8 02 01 00 33 c0 e8 6a 01 68 01 00 00 7f ff 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 30 00 00 00 73 00 2e 00 73 00 79 00	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 d0 e8 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83	68 60 13 01 00 6a 05 6a 0a 00 00 85 00 5 00 63 00 65 00 5c 00 43 00 6c 00 61 00 73 00 6c 00 61 00 73 00 ec 14 53 68 4e 07 01	3. TSh`i. j.n52ju[.\.D.e.v.i.c.e.\. K.e.y.b.o.a.r.d.C.l.a.s .s.0k.b.d.c.l.a.s. ss.y.sUShN.
702 719 730 747 75E 775 78C 783	5d e0 74 18 80 7d e7 01 15 d8 02 01 00 33 c0 e8 6a 01 68 01 00 00 71 11 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 30 00 00 00 00 73 00 2e 00 73 00 79 00 00 8d 45 ec 50 32 db ff	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 a0 e8 00 44 00 65 00 76 00 64 00 66 00 61 00 72 00 64 00 00 66 00 62 00 64 00 63 73 00 00 00 55 86 ec 83 15 d4 02 01 00 8d 45 f8	68 60 13 01 00 6a 05 6a 0a 00 00 85 00 75 00 63 00 65 00 5c 00 43 00 6c 00 61 00 73 00 6c 00 61 00 73 00 ec 14 53 68 4e 07 01 50 8d 45 f4 50 68 00	3. TSh`i. j.n52. juE.\D.e.v.i.c.e.\ K.e.y.b.o.a.r.d.C.l.a.s .s.0k.b.d.c.l.a.s ss.y.sUShNE.P2E.P.E.Ph
702 719 730 747 75E 775 780 783 788	5d e8 74 18 88 7d e7 01 15 d8 82 81 88 33 c8 e8 88 81 85 81 80 80 77 17 17 82 6 c3 8a c3 5b c3 5c 4b 86 65 88 63 5b 62 80 80 73 80 80 80 80 80 80 73 80 26 80 73 80 26 65 80 73 80 45 6c 50 32 db ff 80 10 80 8d 45 ec 50 ff	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 qp e8 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 8d 45 f8 15 b8 02 01 00 85 c0 0f	68 60 13 01 00 6a 05 6a 0a 00 00 85 00 75 00 63 00 65 00 5c 00 43 00 6c 00 61 00 73 00 6c 00 61 00 73 00 6c 00 61 00 73 01 45 3 68 4e 07 01 50 8d 45 f4 50 68 00 85 a0 01 00 00 39 45	3. TSh`i. J.n52. Jt[\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
702 719 730 747 75E 775 78C 7A3 7BA 7D1	5d e8 74 18 88 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 6b 01 00 00 71 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 79 00 00 8d 45 ec 50 32 db ff 60 10 00 8d a4 a4 01 00 00 39	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 8d 45 f8 15 b8 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00	68 68 13 81 88 68 85 68 68 88 88 88 88 88 88 88 88 88 88 88	
702 719 730 747 75E 775 780 783 788	5d e8 74 18 88 7d e7 01 15 d8 82 81 88 33 c8 e8 88 81 85 81 80 80 77 17 17 82 6 c3 8a c3 5b c3 5c 4b 86 65 88 63 5b 62 80 80 73 80 80 80 80 80 80 73 80 26 80 73 80 26 65 80 73 80 45 6c 50 32 db ff 80 10 80 8d 45 ec 50 ff	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 qp e8 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 8d 45 f8 15 b8 02 01 00 85 c0 0f	68 60 13 01 00 6a 05 6a 0a 00 00 85 00 75 00 63 00 65 00 5c 00 43 00 6c 00 61 00 73 00 6c 00 61 00 73 00 6c 00 61 00 73 01 45 3 68 4e 07 01 50 8d 45 f4 50 68 00 85 a0 01 00 00 39 45	3. TSh`i. J.n52. Jt[\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
702 719 730 747 75E 775 78C 7A3 7BA 7D1 7E8 7FF 816	5d e8 74 18 88 7d e7 81 15 d8 82 81 88 32 68 e8 84 84 84 84 84 84 84 84 86 86 86 86 86 86 86 86 86 86 86 86 86	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 d0 e8 00 44 00 65 00 76 00 64 00 66 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 8d 45 f8 15 b8 02 01 00 85 c0 0f 45 f8 0f 80 48 e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c	68 60 13 01 00 6a 05 6a 0a 00 00 85 00 75 00 63 00 65 00 5c 00 43 00 6c 00 61 00 73 00 6c 00 61 00 73 00 ec 14 53 68 4e 07 01 50 8d 45 f4 50 68 00 85 a0 01 00 00 39 45 ff 75 f4 e8 75 08 00 00 8b 48 04 8b 49 60 00 00 8b 45 fc 8b 55 50 ff 91 38 01 00 00	
702 719 730 747 75E 775 78C 7A3 7BA 7D1 7E8 7FF 816 82D	5d e8 74 18 88 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 6b 01 00 00 77 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 00 00 00 00 00 00 8d 45 ec 50 32 db ff 00 10 00 8d 45 ec 50 32 db ff 14 01 84 a4 01 00 00 39 00 85 c0 89 45 f8 01 84 8d 55 fc 52 50 ff 51 2c f8 8b 52 08 8b 48 04 ff 8d c0 59 59 0f 8d 24 01	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 50 0f 8b 5e 00 00 00 8b 55 f8 8b 45 fc	68 68 13 81 88 68 85 68 68 88 88 88 88 88 88 88 88 88 88 88	
702 719 730 747 75E 775 78C 783 7BA 7D1 7E8 7FF 816 82D 844	5d e8 74 18 88 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 68 01 00 00 77 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 79 00 00 8d 45 ec 50 32 db ff 60 10 00 8d 45 ec 50 6f f4 0f 84 a4 01 00 00 39 00 85 c0 89 45 f8 0f 84 8d 55 fc 52 50 ff 51 2c f8 8b 52 08 8b 48 04 ff 84 c0 59 59 9f 84 24 01 49 04 8b 49 0c 83 c2 44	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 0f 15 b8 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 00 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00	68 68 13 81 88 68 85 68 68 88 88 88 88 88 88 88 88 88 88 88	
702 719 730 747 75E 775 78C 783 78A 7D1 7E8 7FF 816 82D 844 85B	5d e8 74 18 88 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 68 01 00 00 7f 17 02 fe c3 8c c3 5c c3 5c c4 60 65 60 79 00 60 00 73 00 30 00 00 00 00 73 00 2e 00 73 00 79 00 00 8d 45 ec 50 ff 60 10 00 40 40 45 ec 50 ff 64 0f 84 a4 01 00 00 39 00 85 c0 89 45 f8 0f 84 8d 55 fc 52 58 ff 51 2c f8 8b 52 08 8b 48 04 ff 84 c0 59 90 ff 84 24 01 49 04 8b 49 0c 83 c2 44 00 00 00 00 8b 45 fc 8b 48	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 e8 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 00 8b 55 f8 8b 49 0c 00 04 8b 49 04 8b 49 0c 68	68 68 13 81 88 68 85 68 63 88 88 88 88 88 88 88 88 88 88 88 88 88	3. TSh`i. j.n52j
702 719 730 747 75E 775 78C 783 7BA 7D1 7E8 7FF 816 82D 844	5d e8 74 18 88 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 68 01 00 00 77 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 79 00 00 8d 45 ec 50 32 db ff 60 10 00 8d 45 ec 50 6f f4 0f 84 a4 01 00 00 39 00 85 c0 89 45 f8 0f 84 8d 55 fc 52 50 ff 51 2c f8 8b 52 08 8b 48 04 ff 84 c0 59 59 9f 84 24 01 49 04 8b 49 0c 83 c2 44	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 0f 15 b8 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 00 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00	68 68 13 81 88 68 85 68 68 88 88 88 88 88 88 88 88 88 88 88	
702 719 730 747 75E 775 78C 793 78A 7D1 7E8 7FF 816 82D 844 858 872	5d e8 74 18 88 7d e7 01 15 d8 02 01 00 33 c8 e8 64 01 68 01 00 00 77 17 17 02 fe c3 84 c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 79 00 00 8d 45 ec 50 32 db ff 60 10 00 8d 45 ec 50 32 db ff 64 0f 84 a4 01 00 00 39 00 85 c0 89 45 f8 0f 84 8d 55 fc 52 50 ff 51 2c 68 8b 52 08 8b 48 04 ff 84 c0 59 59 69 8d 48 6d 5f 6d 48 38 01 00 00 84 c0 59 59 8b 49 0c 88 0d 80 00 00 8b 45 fc 8b 48 00	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 d0 e8 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 8d 45 f8 15 b8 02 01 00 8d 45 f8 15 b8 02 01 00 8d 25 60 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 00 8b 45 0f 84 db 00 00 00 8b 45	68 60 13 01 00 6a 05 ba 0a 00 00 85 c0 75 00 63 00 65 00 5c 00 43 00 6c 00 61 00 73 00 6c 00 61 00 73 00 ec 14 53 68 4e 07 01 50 8d 45 f4 50 68 00 85 a0 01 00 00 39 45 ff 75 f4 e8 75 08 00 00 8b 48 04 8b 49 0c 00 00 8b 45 fc 8b 55 50 ff 91 38 01 00 00 85 52 08 8b 48 04 8b 84 c0 59 59 0f 84 fd 30 06 01 00 50 ff 91 fc 8b 48 04 8b 49 04	3. I Sh`.i. J.nS2. J0[.\\D.e.v\i.c.e.\\ K.e.y.b.o.a.r.d.C.1.a.s .s.0k.b.d.c.1.a.s ss.y.sUShN E.P2E.P.E.Ph969EU.UE.CH.IU.RP.Q., YY.^\E.UR.H.rD.I.I.P.8YY.\$.U.E.R.H. I.I.DRP.8YYE.H.I.I.h0.P. 8YYE.H.I.I.h0.P.
702 719 730 747 75E 775 78C 783 78A 701 7E8 7FF 816 82D 844 85B 872 889 880 887	5d e8 74 18 88 7d e7 81 15 d8 82 81 80 33 c8 e8 84 80 168 81 80 80 7d e7 81 82 84 84 84 84 84 84 84 84 84 84 84 84 84	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 00 00 00 8b 55 f8 8b 49 00 00 00 8b 55 f8 8b 49 00 66 84 db 00 00 00 8b 45 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 68 0f 84 db 00 00 00 8b 45 50 ff 91 c0 01 00 00 04 8b 49 04 8b 49 06 68 06 84 db 00 00 00 00 8b 45	68 68 13 81 88 68 85 68 68 88 88 88 88 88 88 88 88 88 88 88	3. I Sh`.i. J.n52. J0[.\\D.e.v\i.c.e.\\ K.e.y.b.o.a.r.d.C.l.a.s s.sk.b.d.c.l.a.s s.s.y.sUShNE.P2E.P.E.Ph99EUU E. ( H. IU.RP.Q., YY.^.E.UR.H.IVY.\$.U.E.R.H.I. I.I.DRP.8YYE.H.I.I.h0P. 8YY. E.H.I. I.h.PYY.
702 719 730 747 75E 775 78C 7A3 7BA 7D1 7E8 7FF 816 82D 844 85B 872 889 8A0 8B7 8CE	5d e8 74 18 88 7d e7 01 15 d8 02 01 08 33 c8 e8 64 01 68 01 00 00 77 17 02 fe c3 84 c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 20 00 73 00 20 00 73 00 20 00 30 00 00 00 00 00 86 45 ec 50 32 db ff 00 10 00 84 45 ec 50 ff f4 0f 84 a4 01 00 00 03 90 85 c0 89 45 f8 0f 84 84 55 fc 52 50 ff 51 2c f8 8b 52 08 8b 48 04 ff 84 c0 59 59 0f 84 24 01 49 04 8b 49 0c 83 c2 44 00 40 00 00 00 8b 45 fc 8b 48 38 01 00 00 84 c0 59 59 8b 49 0c 68 01 00 08 00 00 8b 45 fc 8b 48 04 00 00	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 8d 45 f8 15 b8 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 48 b49 04 8b 49 0c 68 0f 84 db 00 00 00 8b 45 50 ff 91 2c 01 00 00 84 8b 49 04 8b 49 0c 68 0f 84 db 00 00 00 8b 45 50 ff 91 2c 01 00 00 84 8b 49 04 8b 49 0c 68 00 00 8b 45 fc 8b 48 04 8d 60 8b 45 fc 8b 48 04	68 68 13 81 88 68 85 68 68 88 89 89 89 85 69 75 80 65 80 56 86 66 86 66 86 66 86 66 86 86 86 86 86	3. I
702 719 730 747 75E 775 78C 7A3 7BA 7D1 7E8 816 82D 844 85B 872 889 8A0 8B7 8CE 8E5	5d e8 74 18 80 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 6b 01 00 00 77 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 2e 00 73 00 79 00 60 00 8d 45 ec 50 32 db ff 00 10 00 8d 45 ec 50 32 db ff 4 01 00 00 83 45 ec 50 6f f 51 2c 68 8b 52 08 8b 48 04 ff 84 c0 59 59 0f 84 24 01 49 04 8b 49 0c 83 c2 44 00 00 00 8b 45 fc 8b 48 38 01 00 00 84 c0 59 59 8b 49 0c 68 01 00 08 00 00 08 8b 45 fc 8b 48 04 84 c0 59 59 0f 84 9a 00 00 00 8b 45 fc 8b 48 04 84 c0 59 59 0f 84 9a 00 00 25 00 ff 91 24 01 00 00 8b 49 0c 6a 01 50 ff 91	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 05 67 67 91 2c 01 00 00 84 8b 49 04 8b 49 0c 6a 00 00 8b 45 fc 50 ff 91 2c 01 00 00 84 8b 49 04 8b 49 0c 6a 00 00 8b 45 fc 50 ff 91 2c 01 00 00 84 8b 49 04 8b 49 0c 6a 00 00 8b 45 fc 8b 48 84 49 04 8b 49 0c 6a 00 00 8b 45 fc 8b 48 84 60 59 59 74 7f 8b 45 24 01 00 00 84 c0 59 59	68 68 13 81 88 68 85 68 68 88 88 88 88 88 88 88 88 88 88 88	3. I Sh i J. I. J. Sh i J. I. J. Sh Sh Z. J Sh I J. I. Sh Z. J
702 719 730 747 75E 775 78C 783 78A 7D1 7E8 7FF 816 82D 844 85B 872 889 887 867 865	5d e8 74 18 88 7d e7 01 15 d8 02 01 00 33 c8 e8 64 01 68 01 00 00 77 17 02 fe c3 84 c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 79 00 60 84 5e c50 32 db ff 00 10 00 85 c0 89 45 f8 0f 84 84 84 55 fc 52 50 ff 51 2c 68 8b 52 08 8b 48 04 ff 84 c0 59 59 0f 84 24 01 49 04 8b 49 0c 83 62 44 00 00 00 8b 45 fc 8b 48 38 01 00 00 84 c0 59 59 8b 49 0c 68 00 00 25 0f ff 91 24 01 00 00 8b 49 0c 68 00 00 8b 49 0c 68 01 50 66 8b 48 04 84 60 59 59 01 84 94 00 00 80 8b 45 fc 8b 48 04 84 60 59 59 01 84 94 00 00 80 84 60 65 00 00 85 65 65 65 65 65 65 65 65 65 65 65 65 65	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 e8 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 05 06 84 86 01 00 00 86 68 68 48 69 00 00 8b 45 50 ff 91 2c 01 00 08 84 8b 49 04 8b 49 0c 6a 00 00 08 8b 45 fc 8b 48 04 8c 05 59 74 7f 8b 45 24 01 00 00 84 c0 59 59 7e 07 01 00 50 ff 91 20	68 68 13 01 00 6a 05 6a 0a 00 00 85 00 5c 00 63 00 65 00 5c 00 63 00 6c 00 61 00 73 00 6c 00 61 00 73 00 ec 14 53 68 4e 07 01 50 8d 45 f4 50 68 00 85 a0 01 00 00 39 45 ff 75 f4 e8 75 08 00 00 8b 48 04 8b 49 0c 00 00 8b 45 fc 8b 55 50 ff 91 38 01 00 00 8b 48 04 8b 48 8b 84 c0 59 59 0f 84 fd 30 06 01 00 50 ff 91 fc 8b 48 04 8b 49 00 50 ff 91 2c 01 00 00 8b 49 04 8b 49 06 6a fc 8b 48 04 8b 49 01 00 08 84 05 59 59	3. I Sh`.i. J.nS2. J0[.\\]D.e.v\i.c.e.\\ K.e.y.b.o.a.r.d.C.1.a.s .s.0k.b.d.c.1.a.s ss.y.sUShN E.P2E.P.E.Ph99EU.UE.CH.I.U.R.P.Q., YY.^E.U.L.R.H.I.I.P.8 YY.\$.U.E.R.H.I.I.D.RP.8YY E.H.I.I.h0.P.8YY 8YY.E.H.I.I.h0.P.8YY 1.I.h.PYY.E.H.I.I.J.P YY.E.H.I.I.J.P YY.E.H.I.I.J.P YY.E.H.I.I.J.P YY.E.H.I.I.J.P YY.E.H.I.I.J.P YY.E.H.I.I.J.P YY.E.H.I.I.J.P YY.E.H.I.I.J.P
702 719 730 747 75E 775 78C 7A3 7BA 7D1 7E8 816 82D 844 85B 872 889 8A0 8B7 8CE 8E5	5d e8 74 18 80 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 6b 01 00 00 77 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 2e 00 73 00 79 00 60 00 8d 45 ec 50 32 db ff 00 10 00 8d 45 ec 50 32 db ff 4 01 00 00 83 45 ec 50 6f f 51 2c 68 8b 52 08 8b 48 04 ff 84 c0 59 59 0f 84 24 01 49 04 8b 49 0c 83 c2 44 00 00 00 8b 45 fc 8b 48 38 01 00 00 84 c0 59 59 8b 49 0c 68 01 00 08 00 00 08 8b 45 fc 8b 48 04 84 c0 59 59 0f 84 9a 00 00 00 8b 45 fc 8b 48 04 84 c0 59 59 0f 84 9a 00 00 25 00 ff 91 24 01 00 00 8b 49 0c 6a 01 50 ff 91	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 05 67 67 91 2c 01 00 00 84 8b 49 04 8b 49 0c 6a 00 00 8b 45 fc 50 ff 91 2c 01 00 00 84 8b 49 04 8b 49 0c 6a 00 00 8b 45 fc 50 ff 91 2c 01 00 00 84 8b 49 04 8b 49 0c 6a 00 00 8b 45 fc 8b 48 84 49 04 8b 49 0c 6a 00 00 8b 45 fc 8b 48 84 60 59 59 74 7f 8b 45 24 01 00 00 84 c0 59 59	68 68 13 81 88 68 85 68 68 88 88 88 88 88 88 88 88 88 88 88	3. I Sh i J. I. J. Sh i J. I. J. Sh Sh Z. J Sh I J. I. Sh Z. J
702 719 730 747 75E 775 78C 7A3 7BA 7D1 7E8 7FF 816 82D 844 85B 872 889 8A0 8B7 8CE 913 92A 941	5d e8 74 18 80 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 6b 01 00 00 7f 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 2e 00 73 00 2e 00 73 00 79 00 60 00 8d 45 ec 50 32 db ff 00 10 00 8d 45 ec 50 32 db ff 4 0f 84 a4 01 00 00 39 00 85 c0 89 45 f6 80 f8 46 65 5c	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 66 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 07 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 48 b 49 04 8b 49 0c 60 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 06 04 8b 49 6c 6a 00 00 08 8b 45 fc 8b 48 8b 49 04 8b 49 0c 6a 00 00 00 8b 55 ff 91 50 50 ff 91 00 50 ff 91 20 8b 49 04 8b 49 0c 6a 00 00 00 8b 65 67 70 01 00 50 ff 91 20 8b 49 04 8b 49 8c 6a 07	68 68 13 01 00 6a 05 6a 0a 00 00 85 00 75 00 63 00 65 00 56 05 43 00 6c 00 61 00 73 00 6c 00 61 00 73 00 ec 14 53 68 4e 07 01 50 8d 45 f4 50 68 00 85 a0 01 00 00 39 45 ff 75 f4 e8 75 08 00 00 8b 48 04 8b 49 0c 00 00 8b 45 fc 8b 55 6 ff 91 38 01 00 00 8b 45 04 8b 44 fd 30 06 01 00 50 ff 6 8b 48 04 8b 49 04 c0 59 59 0f 84 fd 30 06 01 00 50 ff 6 8b 48 04 8b 49 04 c0 59 59 0f 84 b9 00 50 ff 91 2c 01 00 00 8b 49 04 8b 49 04 6c 8b 48 04 8b 49 04 74 64 8b 45 fc 8b 48 01 00 00 84 c0 59 59 68 31 c4 00 00 68 01 20 8b 45 fc 8b 48 04 00 00 84 c0 59 59 74	3. I Sh i J.n S Z. J U [N.D.e.v.i.c.e.\ K.e.y.b.o.a.r.d.C.1.a.s s.s.0k.b.d.c.1.a.s s.s.y.s. U. ShN. E.P2
702 719 730 747 75E 775 76C 7A3 7BA 7D1 7E8 82D 844 85B 872 889 8A0 8B7 8CE 8E5 8FC 913 92A 941	5d e8 74 18 88 7d e7 01 15 d8 02 01 00 33 c8 e8 63 01 68 01 00 00 77 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 2e 00 73 00 00 00 00 00 00 00 00 8d 45 ec 50 32 db ff 00 10 00 85 c0 89 45 f8 0f 84 8d 55 fc 52 50 ff 51 2c 68 8b 52 08 8b 48 04 ff 84 c0 59 59 0f 84 24 01 49 04 8b 49 0c 68 74 46 8b 45 fc 8b 48 04 66 57 4 46 8b 45 fc 8b 48 04 00 77 50 ff 91 04 8b 49 04 8b 49 0c 68 74 46 8b 45 fc 8b 48 04 00 07 75 07 ff 91 e0 08 8b 49 0c 68 74 46 8b 45 fc 8b 48 04 66 87 49 04 8b 49 0c 68 74 46 8b 45 fc 8b 48 04 8b 49 0c 68 74 6c 68 74 8b 49 0c 68 74 8b 49 6c 6	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 80 f8 4 db 00 00 00 8b 45 50 ff 91 2c 01 00 08 48 8b 49 04 8b 49 0c 6a 00 00 8b 45 fc 8b 48 04 8c 05 59 74 7f 8b 45 24 01 00 00 84 c0 59 59 7e 07 01 00 50 ff 91 20 8b 49 04 8b 49 0c 6a 07 00 00 83 c4 10 85 c0 75 13 01 00 50 ff 91 bc 01 04 8b 40 04 8b 49 6c 6a 07	68 68 13 81 88 68 85 68 75 88 88 89 89 88 85 69 75 89 65 89 56 75 89 66 89 66 89 66 89 66 89 66 89 66 89 67 81 58 88 88 89 89 89 89 89 89 89 89 89 89 89	3. I Sh i J. I. J. Sh i J. I. J. Sh Sh I J. Sh
702 719 730 747 75E 775 78C 783 78A 701 7E8 7FF 816 820 844 858 872 889 880 887 865 867 865 872 889 899 809 809 809 809	5d e8 74 18 80 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 68 01 00 00 77 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 30 00 00 00 00 73 00 2e 00 73 00 79 00 00 8d 45 ec 50 32 db ff 00 10 00 8d 45 ec 50 ff f4 0f 84 a4 01 00 00 39 00 85 fc 52 50 ff 51 2c f8 8b 52 08 8b 48 04 ff 84 c0 59 59 0f 84 24 01 49 04 8b 49 0c 83 c2 44 00 00 00 86 45 fc 8b 48 38 01 00 00 84 c0 59 59 8b 49 0c 68 01 00 08 00 00 85 66 01 50 ff 91 49 04 8b 49 0c 68 74 46 8b 45 fc 8b 48 04 00 00 7f 50 ff 91 e0 00 8b 49 06 68 74 46 8b 45 45 fc 8b 48 00 00 7f 50 ff 91 e0 00 8b 49 06 68 74 46 8b 45 45 fc 8b 48 00 00 7f 50 ff 91 e0 00 8b 49 06 68 74 46 8b 45 45 fc 8b 48 00 00 7f 50 ff 91 e0 00 8b 49 06 68 74 46 8b 45 fc 8b 48 00 00 7f 50 ff 91 e0 00 8b 49 06 68 74 46 8b 45 fc 8b 48 04 8b 49 06 68 74 66 8f 66 87 06 66 77 07 70 70 70 70 70 70 70 70 70 70 70 70 7	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 66 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c8 0f 15 b8 02 01 00 85 c8 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 68 0f 84 db 00 00 00 8b 45 50 ff 91 2c 01 00 08 44 8b 49 04 8b 49 0c 6a 00 00 08 8b 45 fc 8b 48 04 84 c0 59 59 74 7f 8b 45 24 01 00 00 84 c0 59 59 7e 07 01 00 50 ff 91 20 8b 49 04 8b 49 0c 6a 07 00 00 83 c4 10 85 c0 75 13 01 00 50 ff 91 bc 01 04 8b 40 04 8b 40 06 8d 15 b0 02 01 00 8a c3 5b	68 68 13 01 00 6a 05 6a 0a 00 00 85 c0 75 00 63 00 65 00 5c 75 00 63 00 65 00 5c 73 00 6c 00 61 00 73 00 ec 14 53 68 4e 07 01 50 8d 45 f4 50 68 00 85 a0 01 00 00 39 45 ff 75 f4 e8 75 08 00 00 8b 48 04 8b 49 0c 00 00 8b 45 fc 8b 55 50 ff 91 38 01 00 00 8b 48 04 8b 48 8b 84 c0 59 59 0f 84 fd 30 06 01 00 50 ff 91 fc 8b 48 04 8b 49 00 50 ff 91 2c 01 00 00 8b 49 04 8b 49 06 6a fc 8b 48 04 8b 49 04 74 64 8b 45 fc 8b 59 68 31 c4 00 00 68 01 20 8b 45 fc 8b 48 04 00 00 84 c0 59 59 68 31 c4 00 00 68 01 20 8b 45 fc 8b 48 04 00 00 84 c0 59 59 66 31 c4 00 00 68 01 20 8b 45 fc 8b 48 04 00 00 84 c0 59 59 66 31 c4 00 00 68 01 20 8b 45 fc 8b 48 04 00 00 84 c0 59 59 66 55 8b ec 83	3. I Sh` i J. N. i J. N. Sh` i J. N. Sh` z z . J
702 719 730 747 75E 775 78C 7R3 7BA 7D1 7E8 7FF 816 82D 844 85B 872 889 8A0 8B7 8CE 8E5 8FC 913 92A 941 958	5d e8 74 18 88 7d e7 81 15 d8 82 81 88 32 68 e8 84 81 88 91 90 90 77 17 19 19 60 62 80 81 81 81 81 81 81 81 81 81 81 81 81 81	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 6f 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 8d 45 88 15 b8 02 01 00 85 c0 0f 45 f8 0f 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 0c 00 08 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 08 48 b49 04 8b 49 0c 68 0f 84 db 00 00 00 8b 45 50 ff 91 2c 01 00 00 84 8b 49 04 8b 49 0c 6a 00 08 8b 55 fc 8b 48 04 8c 68 59 59 74 7f 8b 45 54 01 00 00 84 c0 59 59 7e 07 01 00 50 ff 91 20 8b 49 04 8b 49 0c 6a 07 00 00 83 c4 10 85 c0 75 13 01 00 50 ff 91 bc 01 04 8b 40 40 8b 60 63 8b 49 64 8b 69 0c 63 15 b0 02 01 00 8a 63 5b 45 f8 50 6a 01 68 01	68 68 13 81 88 68 85 68 68 88 88 88 88 88 88 88 88 88 88 88	3. T. Sh. i.  J.n. S. Z. J  K.e.y.b.o.a.r.d.C.1.a.s. s.0k.b.d.c.1.a.s. s.s.y.s. U. ShN. E.P2E.P.E.Ph. E.P9E U.R.P.Q. YY.^ E. U. U. R. H. I. J.P. 8. YY. \$. U.E. R. H. I. J. DRP. 8. YY. E. H. I. J. P. 8. YY E. H. I. J. J. P. YY. E. H. J. J. P. YY. E. H. I. J. J. P. S. YY. E. H. J. J. J. P. YY. E. H. I. J. J. P. S. YY. L. J. J. P. S. YY E. H. J. J. J. J. P. S. YY E. H. J. J
702 719 730 747 75E 775 78C 783 78A 701 7E8 7FF 816 820 844 858 872 889 880 887 865 867 865 872 889 899 809 809 809	5d e8 74 18 88 7d e7 81 15 d8 82 81 88 32 68 e8 84 81 88 91 90 90 77 17 19 19 60 62 80 81 81 81 81 81 81 81 81 81 81 81 81 81	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 66 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 06 15 b8 02 01 00 85 c0 06 45 18 06 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 06 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 68 0f 84 db 00 00 00 8b 45 50 ff 91 2c 01 00 08 44 8b 49 04 8b 49 0c 6a 00 00 08 8b 45 fc 8b 48 04 8b 49 04 8b 49 06 6a 00 00 08 8b 45 fc 8b 48 04 8b 49 08 8b 49 06 6a 00 00 00 8b 45 fc 8b 48 04 8b 49 08 8b 49 06 6a 07 7e 07 01 00 50 ff 91 20 8b 49 04 8b 49 06 6a 07 00 08 83 c4 10 85 c0 75 13 01 00 50 ff 91 bc 01 04 8b 40 04 8b 40 8c 8d 15 b0 02 01 00 8a c3 5b 45 f8 50 6a 01 68 01 00 b3 08 00 00 85 c0 75 26	68 68 13 01 00 6a 05 6a 0a 00 00 85 c0 75 00 63 00 65 00 5c 75 00 63 00 66 00 61 00 73 00 6c 00 61 00 73 00 ec 14 53 68 4e 07 01 50 8d 45 f4 50 68 00 85 a0 01 00 00 39 45 ff 75 f4 e8 75 08 00 00 8b 48 04 8b 49 0c 00 00 8b 45 fc 8b 55 50 ff 91 38 01 00 00 8b 48 04 8b 48 04 8c 05 59 59 0f 84 fd 30 06 01 00 50 ff 91 fc 8b 48 04 8b 49 04 c0 59 59 0f 84 90 c0 59 59 0f 84 60 30 06 01 00 50 ff 91 fc 8b 48 04 8b 49 04 c0 59 59 0f 84 90 c0 59 59 0f 84 69 c0 59 59 0f 84 74 c0 59 59 0f 84 59 c0 59 67 64 59 60 c0 59 59 0f 84 69 c0 59 59 67 c0 59 59 68 c0 59 59 68 c0 59 59 59 c0 60 60 60 c0 60 60 c0 60 60 60 c0 60 c0 60	3. T. Sh. i. J.n S. Z. J t [.\.] D.e. v.i.c.e.\ K.e.y.b.o.a.r.d.C.1.a.s .s.0k.b.d.c.1.a.s ss.y.s. U. ShNE.P2
702 719 730 747 75E 775 78C 783 78A 7D1 7E8 7FF 816 820 844 858 872 889 880 887 865 867 865 913 92A 941 958 966 990 984	5d e8 74 18 80 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 68 01 00 00 77 17 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 30 00 00 00 00 73 00 26 00 73 00 79 00 00 8d 45 ec 50 32 db ff 00 10 00 8d 45 ec 50 ff f4 0f 84 a4 01 00 00 39 00 85 fc 52 50 ff 51 2c f8 8b 52 08 8b 48 04 ff 84 c0 59 59 0f 84 24 01 49 04 8b 49 0c 83 c2 44 40 00 00 86 45 fc 8b 48 38 01 00 00 84 c0 59 59 8b 49 0c 68 01 00 08 00 00 85 66 01 50 ff 91 04 8b 49 04 8b 49 06 05 50 ff 91 24 01 00 00 06 8b 45 fc 8b 48 04 07 50 ff 91 24 01 00 00 08 60 00 85 65 65 65 65 65 07 46 8b 49 04 8b 49 06 68 74 46 8b 45 fc 8b 48 04 08 07 f 50 ff 91 e0 00 8b 49 06 68 74 46 8b 48 56 68 74 08 06 75 50 ff 91 e0 00 8b 40 06 53 64 55 fc 8b 48 00 06 75 50 ff 91 e0 00 8b 40 66 85 ff 00 32 db e8 00 07 51 45 50 10 00 75 14 57 01 00 75 19 90 00 84 40 65	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 66 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 06 15 b8 02 01 00 85 c0 06 45 18 06 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 06 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 68 0f 84 db 00 00 00 8b 45 50 ff 91 2c 01 00 08 44 8b 49 04 8b 49 0c 6a 00 00 08 8b 45 fc 8b 48 04 8b 49 04 8b 49 06 6a 00 00 08 8b 45 fc 8b 48 04 8b 49 08 8b 49 06 6a 00 00 00 8b 45 fc 8b 48 04 8b 49 08 8b 49 06 6a 07 7e 07 01 00 50 ff 91 20 8b 49 04 8b 49 06 6a 07 00 08 83 c4 10 85 c0 75 13 01 00 50 ff 91 bc 01 04 8b 40 04 8b 40 8c 8d 15 b0 02 01 00 8a c3 5b 45 f8 50 6a 01 68 01 00 b3 08 00 00 85 c0 75 26	68 68 13 01 00 6a 05 6a 0a 00 00 85 c0 75 00 63 00 65 00 5c 75 00 63 00 66 00 61 00 73 00 6c 00 61 00 73 00 ec 14 53 68 4e 07 01 50 8d 45 f4 50 68 00 85 a0 01 00 00 39 45 ff 75 f4 e8 75 08 00 00 8b 48 04 8b 49 0c 00 00 8b 45 fc 8b 55 50 ff 91 38 01 00 00 8b 48 04 8b 48 04 8c 05 59 59 0f 84 fd 30 06 01 00 50 ff 91 fc 8b 48 04 8b 49 04 c0 59 59 0f 84 90 c0 59 59 0f 84 60 30 06 01 00 50 ff 91 fc 8b 48 04 8b 49 04 c0 59 59 0f 84 90 c0 59 59 0f 84 69 c0 59 59 0f 84 74 c0 59 59 0f 84 59 c0 59 67 64 59 60 c0 59 59 0f 84 69 c0 59 59 67 c0 59 59 68 c0 59 59 68 c0 59 59 59 c0 60 60 60 c0 60 60 c0 60 60 60 c0 60 c0 60	3. I Sh i J.n. S. Z. J
702 719 730 747 75E 775 78C 7A3 7BA 7D1 7E8 7FF 816 82D 844 85B 872 889 8A0 8B7 8CE 913 92A 941 958 96F 986 99D	5d e8 74 18 80 7d e7 01 15 d8 02 01 00 33 c8 e8 6a 01 68 01 00 00 07 71 02 fe c3 8a c3 5b c3 5c 4b 00 65 00 79 00 62 00 00 73 00 30 00 00 00 00 73 00 2e 00 73 00 79 00 00 8d 45 ec 50 32 db ff 00 10 00 8d 45 ec 50 6f f4 0f 84 a4 01 00 00 39 00 85 c0 89 45 f8 0f 84 8d 55 fc 52 50 ff 51 2c f8 8b 52 08 8b 48 04 ff 84 c0 59 59 0f 84 24 01 49 04 8b 49 0c 83 c2 44 00 00 00 8b 45 fc 8b 48 38 01 00 00 84 c0 59 59 8b 49 0c 68 01 00 08 00 00 08 8b 45 fc 8b 48 04 c0 59 59 0f 84 24 01 49 04 8b 49 0c 83 c2 44 00 00 00 8b 45 fc 8b 48 00 00 8b 45 fc 8b 48 00 00 00 8b 45 fc 8b 48 00 00 8b 45 fc 8b 48 00 00 8b 45 fc 8b 48 00 00 75 50 ff 91 e0 00 8b 49 0c 6a 01 50 ff 91 04 8b 49 0d 8b 49 0c 68 74 46 8b 45 fc 8b 48 04 00 07 f5 50 ff 91 e0 00 8b 49 0d 8b 49 6c 68 74 46 8b 45 fc 8b 48 04 04 64 85 c9 74 06 ff ec 0c 53 8b 45 fc 8b 40 8b 4d 6d 85 ff 6d 5d 45 00 c6 45 ff 0d 32 db e8 00 75 14 57 01 00	54 08 00 00 c2 10 00 53 35 a0 13 01 00 32 00 68 00 44 00 65 00 76 00 69 66 00 61 00 72 00 64 00 00 6b 00 62 00 64 00 63 73 00 00 00 55 8b ec 83 15 d4 02 01 00 85 c0 06 15 b8 02 01 00 85 c0 06 45 18 06 84 8e 01 00 00 7b 01 00 00 a1 a0 13 01 84 c0 59 59 0f 84 5e 01 72 44 8b 49 04 8b 49 06 00 00 8b 55 f8 8b 45 fc 52 50 ff 91 38 01 00 00 04 8b 49 04 8b 49 0c 68 0f 84 db 00 00 00 8b 45 50 ff 91 2c 01 00 08 44 8b 49 04 8b 49 0c 6a 00 00 08 8b 45 fc 8b 48 04 8b 49 04 8b 49 06 6a 00 00 08 8b 45 fc 8b 48 04 8b 49 08 8b 49 06 6a 00 00 00 8b 45 fc 8b 48 04 8b 49 08 8b 49 06 6a 07 7e 07 01 00 50 ff 91 20 8b 49 04 8b 49 06 6a 07 00 08 83 c4 10 85 c0 75 13 01 00 50 ff 91 bc 01 04 8b 40 04 8b 40 8c 8d 15 b0 02 01 00 8a c3 5b 45 f8 50 6a 01 68 01 00 b3 08 00 00 85 c0 75 26	68 68 13 81 88 68 85 68 68 88 88 88 88 88 88 88 88 88 88 88	3. I Sh i J. I. J. I. J. I. J. I. Sh S. Z. J. Sh

大部分共享代码用于访问系统键盘驱动程序。



```
DeviceKeyboardclass0
                                                                                                                                                                                                                                                                                                                          00010660 DeviceKeyboardclass0:
                                                                                                                       unicode 0, <\Device\KeyboardClass0>,0
db 2 dup(0)
                                                                                                                                                                                                                                                                                                                                                                                                                                           unicode 0, <\Device\KeyboardClass0>,0
align 10h
                                                     unicode 0, <kbdclass.sys>,0

S U B R O U T I N E

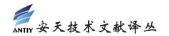
Attributes: bp-based frame

ib_107A0 proc_pear
                                                                                                                                                                                                                                                                                                                                                                 Kbdclass_sys:
                                              Kbdclass_sys:
                                                                                                                                                                                                                                                                                                               | O00106AA | Control | Substitution 
                                                                                                                                                                                                                                                                                                                                                                                                                                unicode 0, <kbdclass.sys>,0
---- SUBROUTINE -----
bp-based frame
    000107A0
000107A0 ; Attributes: bp-Daseu | 1 mm | 1 m
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 CODE XREF: sub
                                                                                                                                                                                                                                              CODE XREF: sub
                                                                                                                                                            ebx
offset DeviceKeyboardclass0 ; Sc
eax, [ebp+DestinationString]
eax ; DestinationStr
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 offset DeviceKeyboardclass0 ; "\
                                                                                                                                                                                                                                                                                                                     000106B1
000106B6
000106B9
000106BA
     000107A7
                                                                                                                        push
lea
                                                                                                                                                                                                                                                                                                                                                                                                                                            push
lea
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                eax, [ebp+DestinationString]
eax ; DestinationStr
     000107AC
                                                                                                                       push
xor
call
lea
push
lea
                                                                                                                                                                                                                                                                                                                                                                                                                                          push
xor
call
lea
push
lea
push
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                eax ; Desti
bl, bl
ds:RtlInitUnicodeString
                                                                                                                                                         000107AF
     00010780
   000107B0
000107B2
000107B8
000107BC
000107BC
                                                                                                                                                                                                                                                                                                                     000106BA
000106BC
000106C2
000106C5
000106C6
000106CA
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 ds:RtlInitUnicodeStrang
eax, [ebp+DeviceObject]
eax ; [ebp+FileObject]
eax ; [ebp+FileObject]
eax ; FileObject
100000h ; DesiredAccess
                                                                                                                        push
    000107C0
                                                                                                                        push
lea
                                                                                                                                                                                                                                                                                                                                                                                                                                           push
lea
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  eax, [ebp+DestinationString]
    000107C5
                                                                                                                                                                                                                                                                                                                        000106CF
                                                                                                                                                                                                                                                                                                                      000106D2
000106D3
000106D9
                                                                                                                                                             eax ; ObjectName
ds:IoGetDeviceObjectPointer
    00010708
                                                                                                                        push
call
test
jnz
cmp
jz
cmp
jz
                                                                                                                                                                                                                                                                                                                                                                                                                                           push
call
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  eax ; ObjectName
ds:IoGetDeviceObjectPointer
    00010709
                                                                                                                                                           ds:IoGetDeviceObjectPointer
eax, eax
loc_lo977
[ebp+FileObject], eax
loc_lo984
[ebp+DeviceObject], eax
loc_lo977
[ebp+FileObject]
IoGetBaseFileObject]
IoGetBaseFileSystemDeviceObject
eax, eax
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                ds:IoGetDeviceObjectPointer
eax, eax
loc_10881
[ebp+FileObject], eax
loc_1088E
[ebp+DeviceObject], eax
loc_10881
[ebp+FileObject]
IoGetBaseFileSystemDeviceObject
    0001 07CF
                                                                                                                                                                                                                                                                                                                     000106D9
000106DB
000106E1
000106E4
000106EA
000106ED
000106F3
    000107CF
000107D1
000107D7
000107DA
000107E0
                                                                                                                                                                                                                                                                                                                                                                                                                                           jnz
cmp
jz
cmp
    000107E3
                                                                                                                                                                                                                                                                                                                                                                                                                                           push
                                                                                                                        push
    000107E9
    000107EC
                                                                                                                        call
                                                                                                                                                                                                                                                                                                                      000106F6
000106FB
                                                                                                                                                                                                                                                                                                                                                                                                                                           call
test
                                                                                                                                                            locetbase=llesystemDevic
eax, eax
[ebp+DeviceObject], eax
loc_10977
eax, dword_ll3CO
ecx, [eax+4]
ecx, [ecx+0Ch]
edx, [ebp+var_4]
edx
    0001 07F1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  eax, eax
[ebp+DeviceObject], eax
                                                                                                                                                                                                                                                                                                                     000106FB
00010700
00010706
00010708
0001070E
00010711
00010714
00010715
00010716
     000107F3
                                                                                                                        mov
jz
mov
mov
mov
lea
                                                                                                                                                                                                                                                                                                                                                                                                                                            mov
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                [ebp+DeviceObject
loc_1088]
eax, dword_11508
ecx, [eax+4]
ecx, [ecx+0Ch]
edx, [ebp+var_4]
edx
   000107F3
000107F6
000107FC
00010801
00010804
00010807
                                                                                                                                                                                                                                                                                                                                                                                                                                          mov
mov
mov
lea
push
    0001080A
                                                                                                                        push
                                                                                                                                                             edx
                                                                                                                       push
call
test
    0001080B
                                                                                                                                                             eax
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                dword ptr [ecx+2Ch]
al, al
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  eax
                                                                                                                                                            dword ptr [ecx+2Ch] al, al
 00010811 00010812 50251.dll (Regin module) 00010812 00010815 00010816 00010816 00010816 00010817 00010817
    00010800
                                                                                                                                                                                                                                                                                                                                                                                                                                            call
                                                                                                                                                                                                                                                                                                                      00010719
                                                                                                                                                                                                                                                                                                                                                                                                                                           test
                                                                                                                                                                                                                                                                                                                     00010719
0001071B
0001071D
00010723
00010726
00010729
0001072C
00010732
00010735
00010738
                                                                                                                                                                                                                                                                                                                                                                20123.sys ("qwerty")
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                edx, [ebp+DeviceObject]
edx, [edx+8]
ecx, [eax+4]
dword ptr [edx+44h]
ecx, [ecx+4]
ecx, [ecx+0ch]
                                                                                                                                                            edx, [edx+8]
edx, [edx+8]
ecx, [eax+4]
dword ptr [edx+44h]
ecx, [ecx+4]
ecx, [ecx+0ch]
                                                                                                                                                                                                                                                                                                                                                                                                                                           mov
push
     00010822
                                                                                                                        mov
     00010825
                                                                                                                        push
    00010828
                                                                                                                         mov
                                                                                                                                                                                                                                                                                                                                                                                                                                            mov
    0001082B
                                                                                                                        push
call
test
    0001082F
                                                                                                                                                                                                                                                                                                                       00010738
                                                                                                                                                                                                                                                                                                                                                                                                                                            push
call
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                eax
dword ptr [ecx+138h]
al, al
ecx
ecx
loc_1086D
                                                                                                                                                            dword ptr [ecx+138h]
al, al
ecx
     00010826
                                                                                                                                                                                                                                                                                                                       00010739
                                                                                                                                                                                                                                                                                                                                                                                                                                           test
pop
pop
jz
                                                                                                                                                                                                                                                                                                                       0001073F
                                                                                                                                                                                                                                                                                                                0001073F
00010741
00010742
00010743
00010749
0001074C
                                                                                                                        pop
                                                                                                                        pop
                                                                                                                         jz
                                                                                                                                                             edx, [ebp+DeviceObject]
eax, [ebp+var_4]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 edx, [ebp+DeviceObject]
eax, [ebp+var_4]
                                                                                                                                                                                                                                                                                                                                                                                                                                             mov
    00010842
                                                                                                                                                                                                                                                                                                                                                                                                                                           mov
```

大部分的 Qwerty 组件从同样的包(插件号码 20121 - 20123)中调用插件,但是有一段代码也存在于 Regin 平台的插件中。这段代码同时存在于 Qwerty 20123 模块和 Regin 50251 模块中,而且寻址 Regin 50225 插件(该插件在 Regin 的虚拟文件系统中)。插件 50225 负责内核模式挂钩。

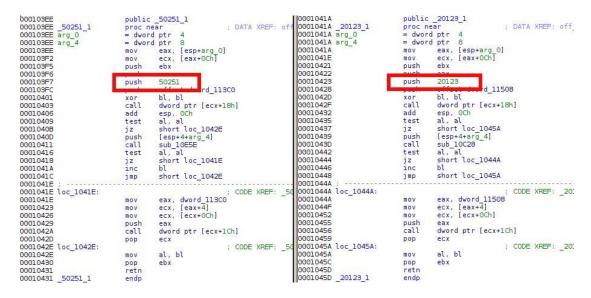
```
0001080F
00010812
00010815
0001081A
0001081B
                                                                                                                                                                                                          ecx, [ecx+4]
ecx, [ecx+0Ch]
offset Kbdclass_sys ; "kbdclass.sys"
                                                                   ecx, [ecx+4]
ecx, [ecx+0Ch]
offset Kbdclass_sys ; "kbdclass
00010908
                                                   mov
push
                                                                  dword ptr [ecx+120h]
al, al
ecx
0001090B
                                                                                                                                                                                                          eax
dword ptr [ecx+120h]
al, al
00010910
                                                   push
00010911
00010917
                                                   call
test
                                                                                                                                        00010821
                                                                                                                                                                                          test
00010919
                                                   pop
                                                                                                                                        00010823
                                                                                                                                                                                          pop
0001091A
                                                   pop
                                                                                                                                        00010824
                                                                                                                                                                                          pop
                                                                                                                                                                                                          ecx
                                                                   ecx
short loc_10963
eax, [ebp+var_4]
ecx, [eax+4]
ecx, [ecx+4]
ecx, [ecx+0Ch]
                                                                                                                                                                                                          short loc 1086D
0001091B
                                                   iz
                                                                                                                                        00010825
00010827
                                                                                                                                                                                          jz
mov
                                                                                                                                                                                                          eax, [ebp+var_4]
ecx, [eax+4]
ecx, [ecx+4]
ecx, [ecx+0Ch]
0001091D
00010920
                                                                                                                                        0001082A
                                                                                                                                                                                          mov
00010923
                                                   mov
                                                                                                                                        00010820
00010926
                                                                                                                                        00010830
                                                                                                                                                                                          mov
00010929
                                                                                                                                       00010833
00010835
0001092B
                                              push
                                                                   50225
                                                                                                                                                                                         push
                                                                                                                                        0001083A
                                                                   deax dword ptr [ecx+0E0h] esp, 10h eax, eax short loc_10963 eax, [ebp+var_4] ecx, [eax+4] ecx, [ecx+6]
                                                   push
call
add
00010935
                                                                                                                                       0001083F
00010840
                                                                                                                                                                                          push
call
                                                                                                                                                                                                          eax
dword ptr [ecx+0E0h]
00010935
00010936
00010936
0001093F
00010941
00010948
00010949
00010949
0001094F
00010955
                                                                                                                                                                                                          dword ptr [ecx+|
esp, 10h
eax, eax
short loc_1086D
eax, [ebp+var_4]
ecx, [eax+4]
ecx, [ecx+4]
ecx, [ecx+0ch]
                                                                                                                                       00010846
                                                                                                                                                                                          add
test
jnz
mov
mov
mov
mov
                                                                                                                                     00010849
0001084B
00010850
00010853
00010856
00010859
0001085E
0001085F
                                                                                                                                                                                       20123 ("Qwerty")
                                                 50251 (Regin)
```

有确实的证据显示,Qwerty插件只能作为Regin平台的一部分运作能够利用插件50225



的内核挂钩功能。

两个模块使用相同软件平台的另一个证据是两个模块按照次序 1 导出的函数。它们包含可在 Regin 其他任何插件中找到的启动代码,并且包括平台中注册的实际插件号,以允许进一步的模块寻址。只有当模块与 Regin 平台 orchestrator 一起使用时,这才是有道理的。



为何这两个模块具有不同的插件 ID , 这一点尚且未知。也许是因为它们由不同的攻击者使用 , 有各自分配的插件 ID 范围。

### 结论

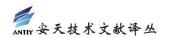
通过分析《明镜周刊》发布的 Qwerty 恶意软件,我们发现它旨在等同于 Regin 平台的一部分。Qwerty 击键记录器不能作为一个独立的模块,它依赖于 Regin 模块 50225 提供的内核挂钩函数。考虑到 Regin 平台的极端复杂性,被不知道源代码的人复制的可能性非常低,所以我们认为 Qwerty 恶意软件开发者和 Regin 开发者是同一伙人或者共同合作。

另一个重要的发现是, Regin 插件存储在加密和压缩的 VFS(虚拟文件系统)之内,这意味着它们并不以"本机"格式直接存在于受害者的机器上。该平台调度器在启动时会加载并执行插件。找到击键记录器的唯一方法是扫描系统内存或解码虚拟文件系统。

## 附录 (MD5)

**QWERTY 20123.sys:** 

0ed11a73694999bc45d18b4189f41ac2



Regin 50251 插件:

c0de81512a08bdf2ec18cb93b43bdc2d

e9a43ea2882ac63b7bc036d954c79aa1