Windows 10 Anniversary更新中hash加密

Passcape Software

1 摘要

微软最近推出了Windows10 Anniversary更新，这是它最流行的操作系统之一。

Windows 10 Anniversary更新使Windows 10比以往任何时候都更好。您可以享受许多新功能，包括：

- 开始菜单中的shuffle按钮
- 利用额外的高要求广告软件的优势
- 调整可爱的磁贴的大小和形状
- 欣赏一下你的个人数据被发送到微软的速度。
- 为那些患有月盲症的人尝试一个出色的单色皮肤
- 查看由数千名辛勤工作的UI设计师开发的全新的极简主义图标
- 花更多的时间在多个窗口中搜索系统选项，从而提高你的超感知觉的标准

然而，严肃地说，这次更新确实带来了一些值得我们关注的重要改进。这些包括Linux shell、纯重新安装、Cortana中改进的智能、基于Windows Hello的新登录选项，等等。

有趣的是，尽管Windows 10的标准登录工作流略有改变，但发行说明中根本没有提到这一点。由于这些微小但重要的更改，大多数用于从Windows中提取密码哈希的黑客工具将不再工作。这些更改可能是由于Microsoft希望停止支持遗留和易受攻击的加密算法。在我们的示例中，Microsoft已决定停止支持RC4。幸运的是，用于审核Windows安全性的最新版本的 Windows密码恢复 已获得对新SAM加密方案的支持。

2 Windows 10 Anniversary更新中hash加密

根据微软的说法，用户密码被存储为哈希值（而不是纯文本表示），可以在Windows注册表的相应部分（仅由系统本身）访问：

HKLM/SAM/SAM/Domains/Account/users/<RID>/V.

其中<RID>-是唯一的用户ID

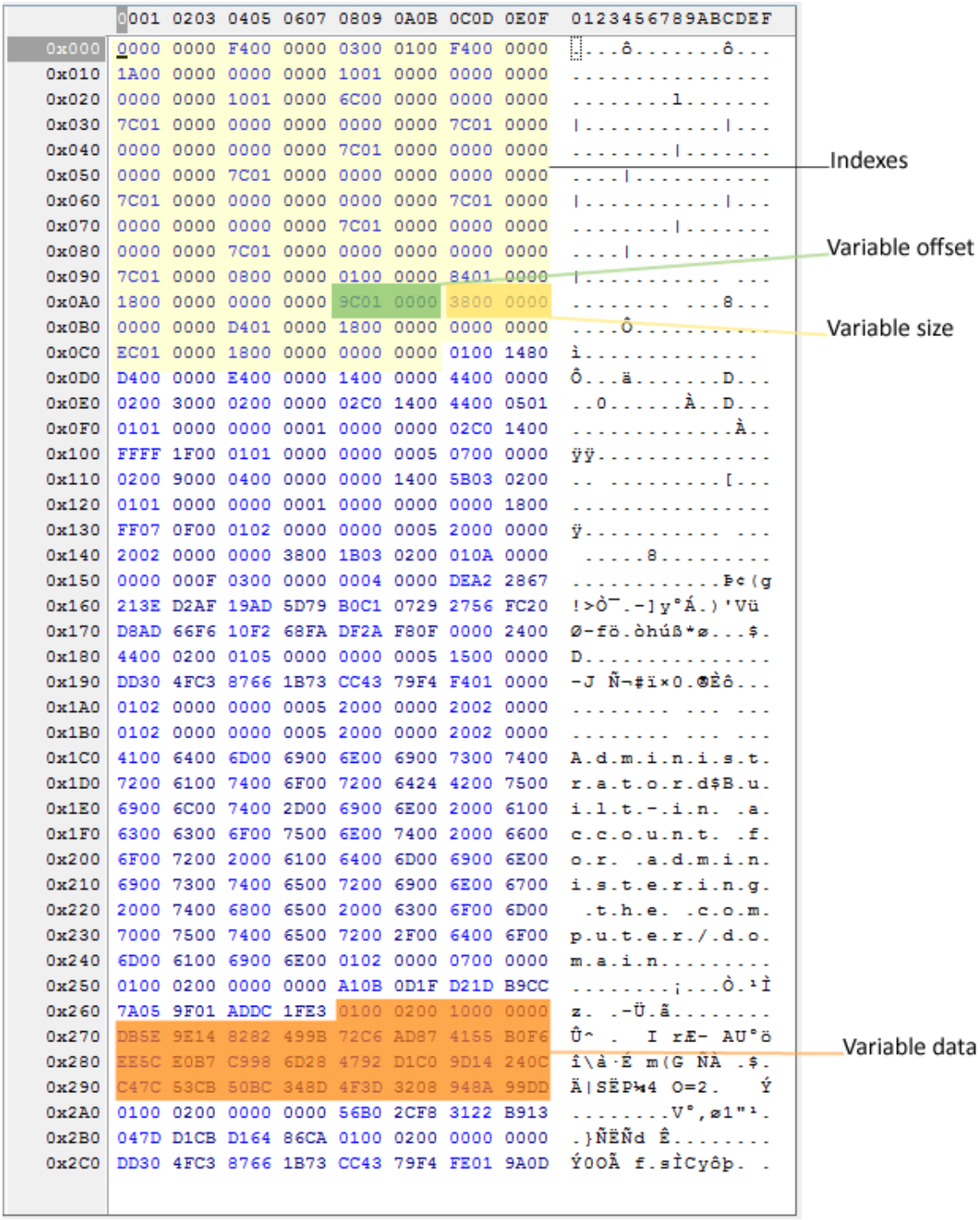
独特的用户ID可以通过扫描以下注册表树来计算出来：

HKLM/SAM/SAM/Domains/Account/users/names/<NAME>

每个包含用户名的密钥都与一个相应的RID相关。例如，管理员账户的RID总是等于500（十六进制符号中的0x1F4），而访客的RID是501（0x1F5）。

任何用户的注册表键也至少有'C'和'V'记录。一个'V'记录包含与该账户相对应的可变长度的数据。这些名称本身似乎是缩写--'V'代表'变量'，'C'意味着'常量'。V'记录中的每个变量都被表示为0到0xCC区间内的一个常数，例如，一个用户名被编码为0xC。因此，如果我们知道这个常数，我们就可以确定

指向实际数据的索引的偏移。LM和NT哈希值分别对应于0x9C和0xA8。然而，获得最终的密码哈希值将需要几个额外的解密步骤。



	0001	0203	0405	0607	0809	0A0B	0C0D	0E0F	0123456789ABCDEF
0x000	0000	0000	F400	0000	0300	0100	F400	0000	....ô.......ô...
0x010	1A00	0000	0000	0000	1001	0000	0000	0000	....
0x020	0000	0000	1001	0000	6C00	0000	0000	0000	........l.......
0x030	7C01	0000	0000	0000	0000	0000	7C01	0000	|...........|...
0x040	0000	0000	0000	0000	7C01	0000	0000	0000	........|.......
0x050	0000	0000	7C01	0000	0000	0000	0000	0000	....|...........
0x060	7C01	0000	0000	0000	0000	0000	7C01	0000	|...........|...
0x070	0000	0000	0000	0000	7C01	0000	0000	0000	........|.......
0x080	0000	0000	7C01	0000	0000	0000	0000	0000	....|...........
0x090	7C01	0000	0800	0000	0100	0000	8401	0000	|........... ...
0x0A0	1800	0000	0000	0000	9C01	0000	3800	0000	....8...
0x0B0	0000	0000	D401	0000	1800	0000	0000	0000	....Ô...........
0x0C0	EC01	0000	1800	0000	0000	0000	0100	1480	ì...............
0x0D0	D400	0000	E400	0000	1400	0000	4400	0000	Ô...ä.......D...
0x0E0	0200	3000	0200	0000	02C0	1400	4400	0501	..0.....À..D...
0x0F0	0101	0000	0000	0001	0000	0000	02C0	1400	..............À..
0x100	FFFF	1F00	0101	0000	0000	0005	0700	0000	ÿÿ..............
0x110	0200	9000	0400	0000	0000	1400	5B03	0200	.. ..[...
0x120	0101	0000	0000	0001	0000	0000	0000	1800	....
0x130	FF07	0F00	0102	0000	0000	0005	2000	0000	ÿ........... ...
0x140	2002	0000	0000	3800	1B03	0200	010A	0000	.....8..........
0x150	0000	000F	0300	0000	0004	0000	DEA2	2867	............Þ¢(g
0x160	213E	D2AF	19AD	5D79	B0C1	0729	2756	FC20	!>Ò¯.-]y°Á.)'Vü
0x170	D8AD	66F6	10F2	68FA	DF2A	F80F	0000	2400	Ø-fö.òhúß*ø...$.
0x180	4400	0200	0105	0000	0000	0005	1500	0000	D...............
0x190	DD30	4FC3	8766	1B73	CC43	79F4	F401	0000	-J Ñ¬#ï×0.ÈÈô...
0x1A0	0102	0000	0000	0005	2000	0000	2002	0000	....
0x1B0	0102	0000	0000	0005	2000	0000	2002	0000	....
0x1C0	4100	6400	6D00	6900	6E00	6900	7300	7400	A.d.m.i.n.i.s.t.
0x1D0	7200	6100	7400	6F00	7200	6424	4200	7500	r.a.t.o.r.d$B.u.
0x1E0	6900	6C00	7400	2D00	6900	6E00	2000	6100	i.l.t.-.i.n. .a.
0x1F0	6300	6300	6F00	7500	6E00	7400	2000	6600	c.c.o.u.n.t. .f.
0x200	6F00	7200	2000	6100	6400	6D00	6900	6E00	o.r. .a.d.m.i.n.
0x210	6900	7300	7400	6500	7200	6900	6E00	6700	i.s.t.e.r.i.n.g.
0x220	2000	7400	6800	6500	2000	6300	6F00	6D00	.t.h.e. .c.o.m.
0x230	7000	7500	7400	6500	7200	2F00	6400	6F00	p.u.t.e.r./.d.o.
0x240	6D00	6100	6900	6E00	0102	0000	0700	0000	m.a.i.n.........
0x250	0100	0200	0000	0000	A10B	0D1F	D21D	B9CC	........¡...Ò.¹Ì
0x260	7A05	9F01	ADDC	1FE3	0100	0200	1000	0000	z. .-Ü.ã........
0x270	DB5E	9E14	8282	499B	72C6	AD87	4155	B0F6	Û^ . I rÆ- AU°ö
0x280	EE5C	E0B7	C998	6D28	4792	D1C0	9D14	240C	î\à·É m(G ÑÀ .$.
0x290	C47C	53CB	50BC	348D	4F3D	3208	948A	99DD	Ä|SËP¼4 O=2. Ý
0x2A0	0100	0200	0000	0000	56B0	2CF8	3122	B913	........V°,ø1"¹.
0x2B0	047D	D1CB	D164	86CA	0100	0200	0000	0000	.}ÑËÑd Ê........
0x2C0	DD30	4FC3	8766	1B73	CC43	79F4	FE01	9A0D	Ý0OÃ f.sÌCyôþ. .

让我们看看系统通常如何检索用户的NTLM hash：

1. 首先，系统确定Windows注册表中存储账户设置的键的路径，例如：HKLM/SAM/SAM/Domains/Account/Users/00001F4
2. 下一步是读取包含NTLM哈希值的变量。这个变量对应的是常数0xA8。因此，系统根据这个常数中的偏移量来读取数据索引，即0x19C。将数据索引加到0xCC，就得到了0x268的偏移量，我们可以从这里访问实际的数据（我们的 "原始 "NTLM哈希值），如图所示。现在系统可以读取哈希值并解密它。
3. 使用SYSKEY，系统解密了SAM会话密钥。SAM会话密钥被存储在名为HKLM/SAM/SAM/Domains/Account/V的注册表部分。这个数据结构实际上保留了两个加密密钥：当前密钥和前一个密钥。在这个步骤中，系统使用MD5和RC4算法。在Windows 10周年更新中，RC4已被AES取代。
4. 然后，系统使用SAM会话密钥，通过RC4或AES（用于Windows 10周年更新）算法解密步骤2中获得的 "原始 "哈希值。
5. 最后，通过DES算法和用户的RID作为加密密钥，将已经获得的数据再次转化为实际数据。现在我们的NTLM哈希值已经准备好了。

如您所见，在Windows 10 Anniversary更新中，步骤3和4中的RC4流密码已替换为AES分组密码。这导致数据存储结构发生了某些变化（至少因为AES块中的数据长度必须是16字节的倍数），但并没有增强操作系统的安全性。

3 总结

在Windows 10 AU中，SAM账户的加密算法已被改变。新算法是否使密码哈希值更安全？不，这值得吗？是的，因为统一的变化也适用于域用户--由于传统的RC4算法的漏洞，他们的一些私人数据有可能被泄露。然而，这完全是另一回事。