विंडोज 10 एनिवर्सरी अपडेट में हैश एन्क्रिप्शन

पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

Table contents

सार

1 सार

Microsoft ने हाल ही में अपने सबसे लोकप्रिय ऑपरेटिंग सिस्टमों में से एक, Windows 10 के लिए एक बड़ा एनिवर्सरी अपडेट पेश किया है।

Windows 10 एनिवर्सरी अपडेट Windows 10 को पहले से बेहतर बनाता है। आप कई नई सुविधाओं का आनंद ले सकते हैं, जिनमें शामिल हैं:

- स्टार्ट मेनू में शफ़ल बटन
- अत्यधिक अनुरोधित अतिरिक्त एडवेयर का लाभ उठाएं
- मनमोहक टाइलों का आकार बदलें और उन्हें नया आकार दें
- प्रशंसा करें कि आपका व्यक्तिगत डेटा कितनी तेज़ी से Microsoft को भेजा जाता है
- मून ब्लाइंडनेस से पीड़ित लोगों के लिए एक शानदार मोनोक्रोम स्किन का प्रयास करें
- हज़ारों मेहनती UI डिज़ाइनरों द्वारा विकसित एकदम नए न्यूनतर चिह्न देखें
- एकाधिक विंडो में सिस्टम विकल्पों की खोज में और भी अधिक समय व्यतीत करें, इस प्रकार आपकी अतिरिक्त संवेदी धारणा के लिए बार बढ़ाएं

हालांकि, गंभीरता से, अपडेट वास्तव में कुछ महत्वपूर्ण सुधार पेश करता है जो हमारे ध्यान देने योग्य हैं। इनमें Linux शेल, प्योर री-इंस्टॉलेशन, Cortana में बेहतर इंटेलिजेंस, विंडोज हैलो पर आधारित नए लॉगिन विकल्प और बहुत कुछ शामिल हैं।

मजेदार बात यह है कि, इस तथ्य के बावजूद कि Windows 10 के मानक लॉगिन वर्कफ़्लो को थोड़ा बदल दिया गया है, रिलीज़ नोट्स में इसका बिल्कुल भी उल्लेख नहीं है। इन मामूली, लेकिन महत्वपूर्ण परिवर्तनों के कारण, विंडोज़ से पासवर्ड हैश निकालने के लिए अधिकांश हैकर टूल अब काम नहीं करेंगे। हो सकता है कि ये परिवर्तन माइक्रोसॉफ्ट की विरासत और कमजोर क्रिप्टोग्राफिक एल्गोरिदम के लिए समर्थन बंद करने की इच्छा से प्रेरित हों। हमारे उदाहरण में, Microsoft ने RC4 के लिए समर्थन बंद करने का निर्णय लिया है। सौभाग्य से, विंडोज पासवर्ड रिकवरी का नवीनतम वर्जन जिसका उपयोग विंडोज सुरक्षा के ऑडिट के लिए किया जाता है, को पहले से ही नई SAM एन्क्रिप्शन योजना के लिए सपोर्ट मिल गया है।

विंडोज 10 एनिवर्सरी अपडेट में हैश एन्क्रिप्शन

2 विंडोज 10 एनिवर्सरी अपडेट में हैश एन्क्रिप्शन

माइक्रोसॉफ्ट के अनुसार, यूजर्स पासवर्ड को हैश (प्लेन-टेक्स्ट प्रतिनिधित्व के बजाय) के रूप में संग्रहीत किया जाता है जिसे विंडोज रजिस्ट्री के संबंधित अनुभाग में एक्सेस किया जा सकता है (केवल सिस्टम द्वारा ही):

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

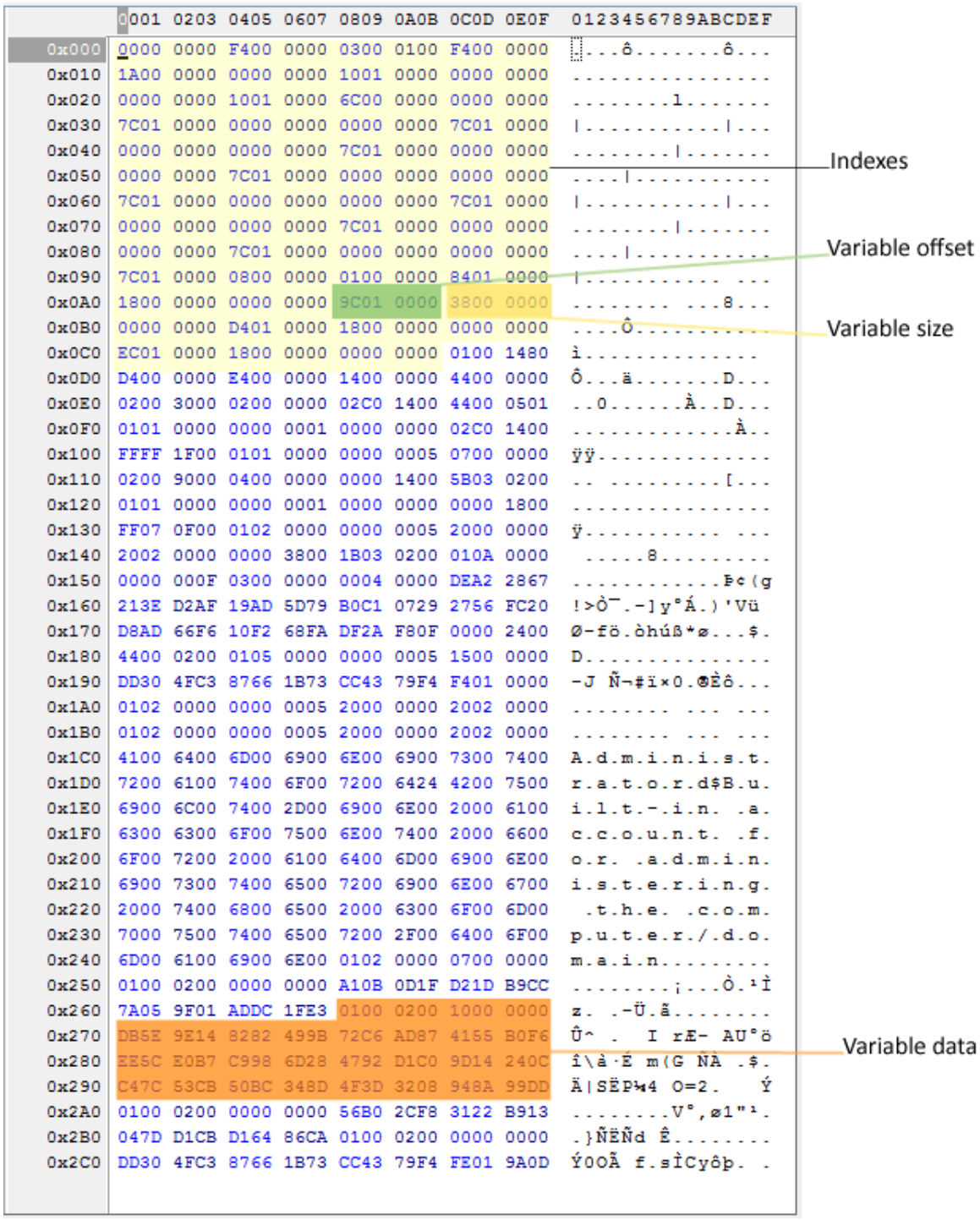
जहां **<RID>** - यूनिक यूजर आईडी है।

निम्नलिखित रजिस्ट्री ट्री को स्कैन करके विशिष्ट यूजर आईडी का पता लगाया जा सकता है:

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

यूजर नाम वाली प्रत्येक की संबंधित RID से जुड़ी होती है। उदाहरण के लिए, व्यवस्थापक खाते का RID हमेशा 500 (हेक्साडेसिमल संकेतन में 0x1F4) के बराबर होता है, जबकि गेस्ट का RID 501 (0x1F5) होता है।

किसी भी यूजर की रजिस्ट्री की में कम से कम 'C' और 'V' रिकॉर्ड भी होते हैं। एक 'V' रिकॉर्ड में वेरिएबल-लेंथ डेटा होता है जो इस अकाउन्ट से संबंधित होता है। नाम स्वयं संक्षिप्त प्रतीत होते हैं - 'V' का अर्थ 'वेरिएबल' और 'C' का अर्थ 'कॉन्स्टन्ट' है। 'V' रिकॉर्ड में प्रत्येक वेरिएबल को 0 से 0xCC के अंतराल के भीतर एक कॉन्स्टन्ट के रूप में दर्शाया जाता है, उदा, एक यूजर नाम 0xC के रूप में एन्कोड किया गया है। इसलिए, यदि हम कॉन्स्टन्ट जानते हैं, तो हम वास्तविक डेटा को संदर्भित करने वाले सूचकांक के लिए एक ऑफसेट की पहचान कर सकते हैं। LM और NT हैश क्रमशः 0x9C और 0xA8 के अनुरूप हैं। हालांकि, अंतिम पासवर्ड हैश प्राप्त करने के लिए कई अतिरिक्त डिक्रिप्शन चरणों की आवश्यकता होगी।



आइए देखें कि सिस्टम आम तौर पर किसी यूजर के NTLM हैश को कैसे पुनः प्राप्त करता है:

1. सबसे पहले, सिस्टम विंडोज रजिस्ट्री में की के पाथ की पहचान करता है जहां अकाउन्ट सेटिंग्स संग्रहीत की जाती हैं, उदा। **HKLM/SAM/SAM/Domains/Account/Users/00001F4**

2. अगला कदम NTLM हैश वाले वेरिएबल को पढ़ना है। यह वेरिएबल कॉन्स्टन्ट 0xA8 से मेल खाता है। इस प्रकार सिस्टम इस कॉन्स्टन्ट, यानी 0x19C में ऑफ़सेट के आधार पर डेटा इंडेक्स को पढ़ता है। डेटा इंडेक्स को 0xCC में जोड़ने से ऑफसेट 0x268 मिलेगा जिससे हम वास्तविक डेटा (हमारे 'कच्चे' NTLM हैश) तक पहुंच सकते हैं जैसा कि चित्र में दिखाया गया है। अब सिस्टम हैश को पढ़ सकता है और उसे डिक्रिप्ट कर सकता है।

3. **SYSKEY** का उपयोग करते हुए, सिस्टम SAM सेशन की को डिक्रिप्ट करता है। SAM सेशन की को **HKLM/SAM/SAM/Domains/Account/V** नामक रजिस्ट्री अनुभाग में संग्रहीत किया जाता है। यह डेटा संरचना वास्तव में दो एन्क्रिप्शन की रखती है: वर्तमान एक और पिछली एक। इस चरण में, सिस्टम **MD5** और **RC4** एल्गोरिदम का उपयोग करता है। विंडोज 10 एनिवर्सरी अपडेट में RC4 को **AES** से रिप्लेस कर दिया गया है।

4. सिस्टम तब RC4 या AES (विंडोज 10 एनिवर्सरी अपडेट के लिए) एल्गोरिथम के माध्यम से चरण 2 में प्राप्त 'कच्चे' हैश को डिक्रिप्ट करने के लिए SAM सेशन की का उपयोग करता है।

5. और, अंत में, जो डेटा प्राप्त किया गया है, उसे एक बार फिर से वास्तविक डेटा में **DES** एल्गोरिथम और यूजर के RID को एन्क्रिप्शन की के रूप में बदल दिया जाता है। अब हमारा NTLM हैश तैयार है।

जैसा कि आप देख सकते हैं, Windows 10 एनिवर्सरी अपडेट में चरण 3 और 4 में **RC4** stream cipher को **AES** block cipher से बदल दिया गया है। इससे डेटा स्टोरेज संरचना में कुछ बदलाव हुए हैं (कम से कम क्योंकि AES ब्लॉक में डेटा की लंबाई 16 बाइट्स से अधिक होनी चाहिए) लेकिन इसके परिणामस्वरूप ऑपरेटिंग सिस्टम की मजबूत सुरक्षा नहीं हुई है।

निष्कर्ष

3 निष्कर्ष

Windows 10 AU में, SAM खातों के एन्क्रिप्शन एल्गोरिदम को बदल दिया गया है। क्या नए एल्गोरिदम ने पासवर्ड हैश को सुरक्षित बना दिया है? नहीं, क्या यह इसके लायक था? हां, चूंकि एकीकृत परिवर्तन डोमेन यूजर्स पर भी लागू होते हैं - उनके कुछ निजी डेटा को विरासती RC4 एल्गोरिथम में कमजोरियों के कारण समझौता होने का खतरा था। हालाँकि, यह पूरी तरह से एक और मामला है।