Jak uzyskać dostęp do historycznego stanu partycji w Windows 7?

16 czerwca 2010

Często zdarza się tak, że chcielibyśmy powrócić do poprzedniej wersji jakiegoś pliku, np. tej sprzed kilku dni. Niewielu użytkowników najnowszego systemu Windows wie o tym, że taka operacja jest jak najbardziej możliwa z wykorzystaniem mechanizmów wbudowanych w sam system. Jeszcze mniej powszechna jest natomiast wiedza na temat tego, że Windows 7 pozwala również na dostęp do jednego z kilku lub nawet kilkunastu historycznych stanów całych partycji! Zobaczmy w jak prosty sposób można tego dokonać.

Dostęp do kilku lub nawet kilkunastu historycznych stanów partycji może się nam przydać w różnych sytuacjach. Będzie to z pewnością nieoceniona pomoc w przypadku poszukiwania poprzedniej wersji określonego pliku lub usuniętego już zbioru. Taka możliwość przyda się jednak również informatykom śledczym prowadzącym cyfrowe dochodzenia lub też… zazdrosnej żonie zainteresowanej zawartością dysku męża sprzed kilku dni, czyli w czasie gdy ona była na kilkudniowym szkoleniu.

Zacznijmy od prostego w użyciu mechanizmu przywracania poprzednich wersji plików, folderów, a nawet całych partycji. W tym celu wystarczy dowolny plik, folder lub też partycję kliknąć prawym przyciskiem myszy i wybrać odpowiednią opcję (niestety dalsze rozważania są słuszne wyłącznie w przypadku Windows 7 Professional, Enterprise oraz Ultimate):

Okazuje się, że w typowym systemie mamy do wyboru nawet kilkanaście historycznych wersji wybranego obiektu (wszystko zależy od bieżącej konfiguracji oraz dostępnego miejsca):

Świetnie, opcja ta na pewno nam się przyda, ale skoro nasz system potrafi przywrócić stan całej partycji sprzed nawet kilkunastu dni, to czy możemy uzyskać dostęp do takiego historycznego widoku stanu partycji, bez przywracania czegokolwiek? Okazuje się, że nie jest to możliwe do wyklinania, jednak przy odrobinie zachodu jest to jak najbardziej wykonalne.

Za okresowe tworzenie kopii w tle wszystkich plików w ramach objętych ochroną partycji w systemie Windows 7 odpowiedzialna jest funkcja Volume Shadow Copy Service – VSS. Poprzednie wersje są zapisywane automatycznie w ramach punktu przywracania, jeśli tylko włączona jest funkcja ochrona systemu. System Windows automatycznie tworzy kopie tylko tych plików i folderów, które zostały zmodyfikowane od momentu utworzenia ostatniego punktu przywracania. Domyślnie punkty przywracania są tworzone raz dziennie, jednak pewne zdarzenia (takie jak zmiana plików systemowych lub instalacja nowych sterowników) mogą wyzwalać utworzenie dodatkowych kopii. Jeśli dysk jest podzielony na partycje lub w komputerze jest więcej niż jeden dysk twardy, domyślnie ochroną plików objęta jest wyłącznie partycja systemowa. Możliwe jest jednak włączenie ochrony w ramach wszystkich pozostałych partycji.

Z technicznego punktu widzenia, VSS monitoruje zmiany zachodzące w ramach danego woluminu na poziomie poszczególnych klastrów, co oznacza, że każda z przechowywanych kopii pozwala nam na odtworzenie wiernego obrazu danej partycji w czasie jej wykonania. Jednak z punktu widzenia informatyka śledczego lub też zazdrosnego małżonka, interesuje nas bardziej dotarcie do wybranego historycznego stanu partycji, bez odtwarzania czegokolwiek.

Zacznijmy od ustalenia listy dostępnych kopii w tle w obrębie interesującej nas partycji. Dla partycji C: możemy w tym celu skorzystać z następującego polecenia: vssadmin list shadows /for=C:. W wyniku tego polecenia otrzymamy listę wszystkich istniejących kopii, warto zwrócić uwagę szczególnie na

informacje takie jak:

– nazwę woluminu kopii w tle (np. HarddiskVolumeShadowCopy4, informację tę znajdziemy w linii: Wolumin kopii w tle: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4),

– czas systemowy w momencie tworzenia kopii w tle (informację tę znajdziemy w linii: Zawierał tyle kopii w tle: 1 w czasie tworzenia: 2009-11-18 09:08:05),

– całkowitą liczbę dostępnych kopii w tle.

Znając już listę dostępnych kopii w tle, możemy przystąpić do analizy zawartych w nich informacji. W celu ręcznego przejrzenia zawartości kopii bezpośrednio z poziomu działającego systemu, najwygodniejsze będzie utworzenie dowiązania symbolicznego do woluminu kopii w tle za pomocą systemowego narzędzia mklink. Przykładowe polecenie może mieć następującą postać: mklink /d C:\kopia_w_tle \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy_nr_kopii\. Polecenie to spowoduje, że za pośrednictwem utworzonego na dysku C: dowiązania o nazwie kopia_w_tle będziemy w stanie swobodnie przeglądać historyczną postać woluminu:

Jak widać, mechanizm tworzenia kopii w tle może nam się przydać do odzyskiwania plików, czy też zbierania informacji o historycznej działalności użytkowników systemu, do którego mamy bezpośredni dostęp. Pamiętajmy jednak o tym, że również ktoś inny może wykorzystać potencjał VSS przeciwko nam samym. O metodach ochrony przed tego typu zagrożeniem pisałem już jednak w jednym z poprzednich artykułów.

Autor: \m/ojtek
Źródło: Hard Core Security Lab