İnformasiya daşıyıcılarından sildiyimiz fayllar həqiqətən də silinirmi?

Tural Məmmədov

Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi, Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi

mammadov.t@cert.gov.az

***Xülasə*— Texnologiyanın inkişafı informasiya daşıyıcılarının çeşidliliyini artırmaqla yanaşı informasiya daşıyıcılarından (kompüter, smartfon, HDD, yaddaş kartları, flash-drive və s.) silinmiş məlumatların bərpa edilməsində də bir çox texnoloji yenilikləri və vasitələri ortaya qoymuşdur. Məqalədə informasiya daşıyıcılarından fayl və məlumatların silinmə prosesinin necə getdiyini, sildiyimizi düşündüyümüz məlumatların əslində silinmədiyini və asanlıqla bərpa oluna biləcəyi izah edilir. Məqalədə gündəlik həyatda istifadə etdiyimiz və yaddaşından sildiyimizi düşündüyümüz informasiya daşıyıcılarının kənar şəxslərin əlinə keçərək informasiya itkisinə səbəb ola biləcək hallar barədə də danışılır.**

Açar sözlər*— *rəqəmsal informasiyanın silinməsi; fayl silmə vasitələri; informasiya daşıyıcıları; yaddaş blokları; məlumatın bərpası; rəqamsal informasiya.

Yəqin ki, banklarda və ya digər mühüm təşkilatlarda sənədlərin necə məhv edildiyinə şahid olmusunuz. Yuxarıdakı şəkildə qismən də olsa bunu göstərmişik. Sənədlər ya yandırılır ya da yuxarıdakı, kimi çox kiçik hissələrə ayrılaraq məhv edilir. Məhvetmədə əsas məqsəd sənədlərin pis niyyətli şəxslərin əlinə keçməməsini təmin etməkdir. Çünki, sənədlər hər nə qədər lazımsız görünsə də ondan faydalanmaq mümkündür. Klassik məhvetmə üsulu öz yerini informasiya daşıyıcılarındakı **(kompüter, smartphone, HDD, yaddaş kartları, flash-drive və s.)** faylların-məlumatların silinməsi-məhvedilməsi üsulları ilə əvəz edilmişdir ki, bu da silinmə üsulunun nə dərəcə də effektiv olması sualını ortaya qoyur.

Bəs görəsən informasiya daşıyıcılarından adi qaydalarla silinən fayllar doğrudanmı silinir?

- Xeyr!

İnformasiya daşıyıcılarından adi qaydada sildiyimiz faylları xüsusi proqram təminatları (recover softs: Easy Recovery, Recuva, Power Data Recovery,TuneUpUtilities, R Studio və s.) vasitəsilə bərpa etmək mümkündür. Məhz bu tip proqram təminatları sistemimizdən silindiyinə inandığımız faylları bərpa edə bilir. Belə nəticəyə gəlmək olar ki, adi qaydada silinmiş olan faylların bərpası o qədər də çətin iş deyil. Bir çoxları diskin format edilməsinin çıxış yolu olduğunu fikirləşirlər. Bu belə deyil. Bu tip proqramlar silinmiş disk bölmələrini (partion, slacks) də bərpa etmək gücünə malikdirlər. Bu səbəbdən də silinməsi lazım olan faylların bu və bu kimi üsullarla silinəcəyinə əmin olmaq yalnışdır.

Bəs fayllarımızı adi qaydalarla sildiyimiz zaman əslində nə baş verir?

Əslində sildiyimiz fayllar sərt diskə baxış zamanı bizə silinmiş kimi görünsə də onlar silinmir. Sadəcə sistemimiz silinməyə daha çox resurs və vaxt sərf etməsin deyə həmin faylın adını və fayla olan keçidini (link) silərək sərt diskdə həmin faylı silinmiş kimi göstərir və həmin faylın həcmini boş yer (free space) kimi qeyd edir. Lakin həmin fayl sərt diskimizdə heç bir yerə köçürülmədən və silinmədən eyni bölmədə saxlanılır. Silinmə əməliyyatı yalnız o zaman başlayır ki, bizim diskimizdəki üzərinə informasiya yazılmamış bütün boş hissələr (partition) dolmuş olsun və növbəti yazacağımız fayllar üçün diskimizdə faktiki boş hissələr olmasın. O zaman sistemimiz yazmaq istədiyimiz yeni informasiyanı daha öncə adını silərək boş göstərdiyi amma faktiki boş olmayan disk hissəsindən silərək onun üzərinə yazacaq. Yəni əgər bizim daha öncə sildiyimiz informasiyanın yerləşdiyi disk hisseciklərinə (slacks) yeni məlumat yazılmayana qədər həmin məlumat olduğu kimi silinmədən qalacaq. Başqa sözlə desək məlumatı silmək üçün mütləq üzərinə başqa bir məlumat yazılmalıdır. Bu vəziyyətlərdə çıxış yolu həmin silmək istədiyiniz sənədin üzərinə ixtiyari (random) məlumatlar yazmaqdır. Yəni diskin format edilməsi və ya faylın SHİFT+DEL+ENTER və ya DEL+ENTER kimi silmə əmrləri çıxış yolu deyil. Bu əməliyyatı həyata keçirmək üçün xüsusi fayl silmə alqoritmləri mövcuddur.

Fayl silmə-məhvetmə vasitərələrindən ən tanınmışları aşağıdakılardır:

-Gutmann(Peter Gutmann) 35 pass
-The DoD 5220.22-M
-NAVSO P5239-26
-PRNG.

Sadalananlardan ən geniş yayılanı Gutmann alqoritmidir. Gutmann texnikası, məlumatı silmək üçün, daha doğrusu yox etmək üçün üzərinə 35 dəfə məlumat yazılmasını nəzərdə tutan bir texnikadır. Normalda silinmiş faylın olduğu yaddaş hissəsinə 1 dəfə tam məlumat yazmaq kifayət etməli idi. Amma

təcrübə bunu sübut etmişdir ki, xüsusi STM (scanning tunneling microscope) adı verilən mikroskop ilə mikroskopik səviyyədə disklərin üzərinə baxış keçirilərsə köhnə məlumatlara azda olsa rast gəlmək mümkündür. Bu kəşfin yaradıcıları Gerd Binnig və Heinrich Rohrer (İBM lab) sonradan Nobel mükafatına layiq görüldülər. STM kvant nəzəriyyəsi qədər dəqiq olaraq kvant mexaniki tunelləmə əsasında yaradılmış atomik səviyyədə mikro məlumatı oxumağa kömək edən cihazdır. Bu tipli laboratoriya şəraiti və istifadə geniş yayılmadığına görə mütəxəssislər keçirtdikləri sınaqlardan sonra silinmiş faylın üzərinə maksimum 6-7 dəfə məlumat yazılmasının kifayət etdiyini bildirmişlər. Əlavə olaraq qeyd edək ki, yuxarıdakı metodlardan istifadədən sonra ələ keçirilən məlumat tam olmur. Yalnız müəyyən bitlər əldə olunur ki, bu da lazımi nəticə üçün kifayət etmir.

Amerika Birləşmiş Ştatları Müdafiə Nazirliyi tərəfindən hazırlanan The DoD 5220.22-M (Department of defence) əsaslandırmasına görə xüsusi gizli məlumatları yox etmək üçün nəzərdə tutulan üsul silinəcək olan məlumatın üzərinə 7 dəfə yazma üsuludur.

File Wipe proqram təminatlarına nümunələr:

http://sourceforge.net/projects/filekiller/
http://www.killdisk.com/downloadfree.htm
http://eraser.heidi.ie/download.php
http://www.dban.org/download

QEYD:

Sildiyinizi düşündüyünüz faylların əslində silinmədiyi və bərpasının asanlıqla mümkün olunduğu informasiya itkisinə (information leackage) səbəb ola biləcək və diqqət tələb edən gündəlik rastlaşdığınız hallar:

- Kompüterin və ya ağıllı telefonunuzun əməliyyat sisteminin yenidən yazılması(format) və ya hər hansı məqsədlə təmiri üçün üçün servisə göndərilməsi;
- Eyni yaddaş ötürücülərinin (flashkart) müxtəlif məqsədlər üçün müxtəlif adamlar tərəfindən istifadəsinə icazə verilməsi;
- Xarab HDD disklərin və ya məlumat daşıyıcılarının fiziki məhv etmədən zibil qutusuna atılması;
- Köhnə kompüterinizi və ya ağıllı telefonunuzu yenisi ilə əvəz etdikdə, köhnənin üzərində təhvil verdiyiniz informasiya daşıyıcıları və sildiyininizi düşündüyünüz məlumatlar və s.

ƏDƏBİYYAT

[1] http://www.east-tec.com/help/predefined-sanitization-standards/
[2] http://www.research.ibm.com/articles/heinrich-rohrer.shtml
[3] http://en.wikipedia.org/wiki/Scanning_tunneling_microscope
[4] http://spiff.rit.edu/classes/phys314/lectures/stm/stm.html