Osiris zsarolóvírus:

A Locky család újabb tagja



## Összefoglaló

Az Acronis olyan új generációs technológiát fejlesztett ki, amely proaktívan megelőzi a nulladik napi fertőzéseket, és lehetővé teszi, hogy a felhasználók váltságdíj kifizetése nélkül akadályozzák meg zsarolóvírusok támadásait és állítsák helyre adataikat. Tegnap a vállalat szakértői felfedezték az Osiris zsarolóvírus egy új mutációját, amely könnyedén megkerülte a Windows Defendert. Tegnap nem volt túl szerencsés napja, de máris van egy új változata, amely ismét kijátszotta a hagyományos biztonsági szoftvereket. Az Acronis Active Protection™ az egyetlen olyan technológia, amely képes az Osiris zsarolóvírus valamennyi verziójának támadásait meggátolni. Sőt, még a titkosított adatok azonnali helyreállítására is képes a zsarolókkal való kapcsolatfelvétel vagy bármilyen váltságdíj kifizetése nélkül. Mindez az Acronis felhővel való integrációnak köszönhető. Az egyetlen trükk az, hogy a zsarolóvírus támadásakor már futnia kell az adott számítógépen.

[A 8 évnyi fontos bizonyíték elvesztéséhez](https://www.scribd.com/document/337573961/Cockrell-Hill-PD-Server-Virus#from_embed) vezető [támadás a Texas állambeli Cockrell Hill-i rendőrség ellen](https://www.theregister.co.uk/2017/01/27/texas_cops_lose_evidence_going_back_eight_years_in_ransomware_attack/) megelőzhető lett volna, ha már telepítették volna az Acronis termékét.

Íme, néhány részlet az új Osiris zsarolóvírus kapcsán:

* Az Osiris a Locky zsarolóvírusok / titkosító vírusok 7. generációja, amely hagyományosan levélszemét-kampányok útján terjed;
* Nehéz észlelni, mivel szabványos Windows összetevőket használ a „payload” (szkriptek és könyvtárak) letöltésére és futtatására;
* Az Osiris beépített virtualizáció-észleléssel rendelkezik, ami megnehezíti a hibakeresést és visszafejtést virtuális gép segítségével; ezt az algoritmust a 2016. júniusi első verzióhoz képest erőteljesen módosították;
* Helyi eszközöket fertőz meg, és könnyedén terjed a hálózaton, hogy újabb számítógépeket és hálózati mappákat fertőzzön meg;
* Az Osiris CRM/Ügyféltámogatási rendszereken (felhő alapúakon is) terjeszthető, szervezeti határokon átívelve is. Az egyik szervezet megfertőzött felhasználója küldhet egy e-mailt egy CRM rendszer e-mail címére; ennek belső parsere elemzi a bejövő e-mailt, és a rosszindulatú csatolmányt egy automatikusan generált jegyre teszi. Az ügyféltámogató szakember megnyitja a jegyet, megnyitja az Excel csatolmányt, és megfertőzi a hálózatot.
* Ahogy azt az Acronis megjósolta, a zsarolóvírusokat alkalmazó bűnöző elkezdték támadni a biztonsági mentési megoldásokat. Az Osiris közvetlenül megtámadja a Microsoft Volume Shadow Copy Service-t (VSS), amely a MS Windows valamennyi példányában megtalálható, és törli a már létrehozott árnyékmásolatokat;
* Az Osiris erős titkosító algoritmusokat alkalmaz, ezért az érintett adatok nem dekódolhatók harmadik fél eszközeivel;
* Érinti a Windows, és valószínűleg a Mac és androidos eszközöket is;

Az integrált biztonsági és biztonsági mentési megoldás kombinációját nyújtó Acronis Active Protection™ képes észlelni és azonnal helyreállítani az Osiris által megtámadott fájlokat.

## A Locky zsarolóvírus-család evolúciója

A Locky zsarolóvírus újabb ráncfelvarráson esett át – kiberbűnözők frissítéseket adtak ki az egyik legelterjedtebb és legkárosabb fájltitkosító zsarolóvírus-családhoz. Az új zsarolóvírus a túlvilág egyiptomi istene után az Osiris nevet kapta, és továbbfejlesztett funkciókkal jelentkezett, melyek célja a biztonsági mentések támadása és az észlelés elkerülése. A vírus a titkosított fájlok nevét a .osiris kiterjesztéssel látja el, és követi a zsarolóvírus-fertőzések szokásos menetrendjét: betör, titkosít, zsarol. A Locky sikerességét meglovagoló Osiris jelenleg a számítógépet használókat fenyegető egyik legkomolyabb kiberbiztonsági fenyegetést jelenti.

A Locky-t először 2016 februárjában fedezték fel, és azóta legalább hét változtatáson esett át, hogy lehetőség szerint egy lépéssel mindig megelőzze az ilyen típusú zsarolóvírusokat észlelni és megállítani igyekvő biztonsági cégeket. A jelek arra mutatnak, hogy a Locky-t eredetileg Oroszországban fejlesztették ki, mivel a korábbi verziók képesek voltak az orosz helyszínre beállított számítógépeket elkerülni. Emellett tartalmaztak olyan Excel-füleket, amelyeken orosz nevek és orosz szleng szavakkal elnevezett szkript-funkciók szerepeltek.

* .locky — 2016. február
* .zepto — 2016. június. Egy hónappal később a Locky elkezdte beágyazott RSA kulcsokkal támogatni az offline titkosítást arra az esetre, ha nem tudna hozzáférni a C&C-khez.
* .odin — 2016. szeptember
* .shit, .thor — 2016. október
* .aesir — 2016. november
* .zzzzz, .osiris — 2016. december

Az Acronis Security Team a következő Osiris zsarolóvírus-mintát vizsgálta:

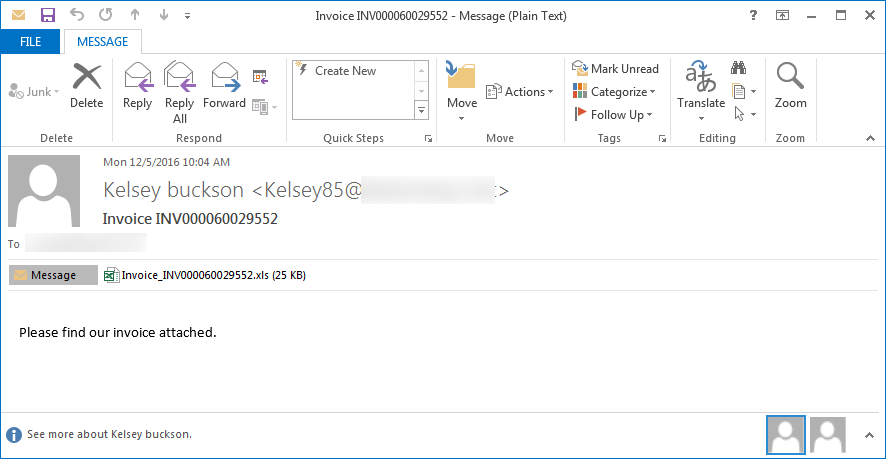
* Fájlnév: ekijLpDlRXB.zk
* Méret: 161625 bájt
* Dátum: 29.01.2017
* MD5: 3545436c22a9a43e29396df87823013d

Megjegyzendő, hogy az Osiris az Apple és az androidos eszközöket is érinti. Az Acronis Security Team jelenleg vizsgálatokat folytat, és külön ki fog adni egy új jelentést.

## Terjedés

**1. LEVÉLSZEMÉT.** Az Osiris zsarolóvírus jellemzően [levélszemét útján](http://www.malware-traffic-analysis.net/2016/12/12/index2.html) terjed. Ezeknek az e-maileknek a tárgysorában az „Invoice” (Számla) vagy az „Order Confirmation” (Megrendelés visszaigazolása) szavak szerepelnek, és tömörített csatolmányuk tartalmazza a rosszindulatú szkriptet. Ez lehet egy Excel-fájl egy VBA makróval vagy egy .jse futtatható szkript (egy „dropper”). Ez futtatáskor letölt egy DLL-fájlt, amelyet a Rundll32.exe segítségével futtat le.

Az Osiris megalkotói úgy próbálják elrejteni a zsarolóvírust, hogy .exe futtatható fájlok helyett szabványos Windows-összetevőket használnak szkriptjeik és DLL fájljaik indítására.



*Példa egy Osiris zsarolóvírussal fertőzött csatolmányt tartalmazó levélszemétre (Fotó: BleepingComputer).*

**2. Rosszindulatú hirdetések („malvertising”).** A zsarolóvírusokat alkalmazó bűnözők legális reklámhálózatokat használnak olyan ügyesen kitalált hirdetések terjesztésére, amelyek csekély felhasználói közreműködéssel, vagy akár anélkül terjesztenek zsarolóvírusokat. A tavaly érintett weboldalak között megtalálható a [BBC, az MSN és az AOL](http://www.theinquirer.net/inquirer/news/2451209/angler-malvertising-ransomware-campaign-is-proving-a-nuisance) is; ezeknél a kiberbűnözők az automatizált reklámhálózatok előnyét kihasználva terjesztettek [rosszindulatú hirdetéseket](https://blog.malwarebytes.com/101/2016/06/malvertising-and-ransomware-the-bonnie-and-clyde-of-advanced-threats/), miután fiókjuk átment a kezdeti ellenőrzéseken.

## Vállalati hálózatok megfertőzése

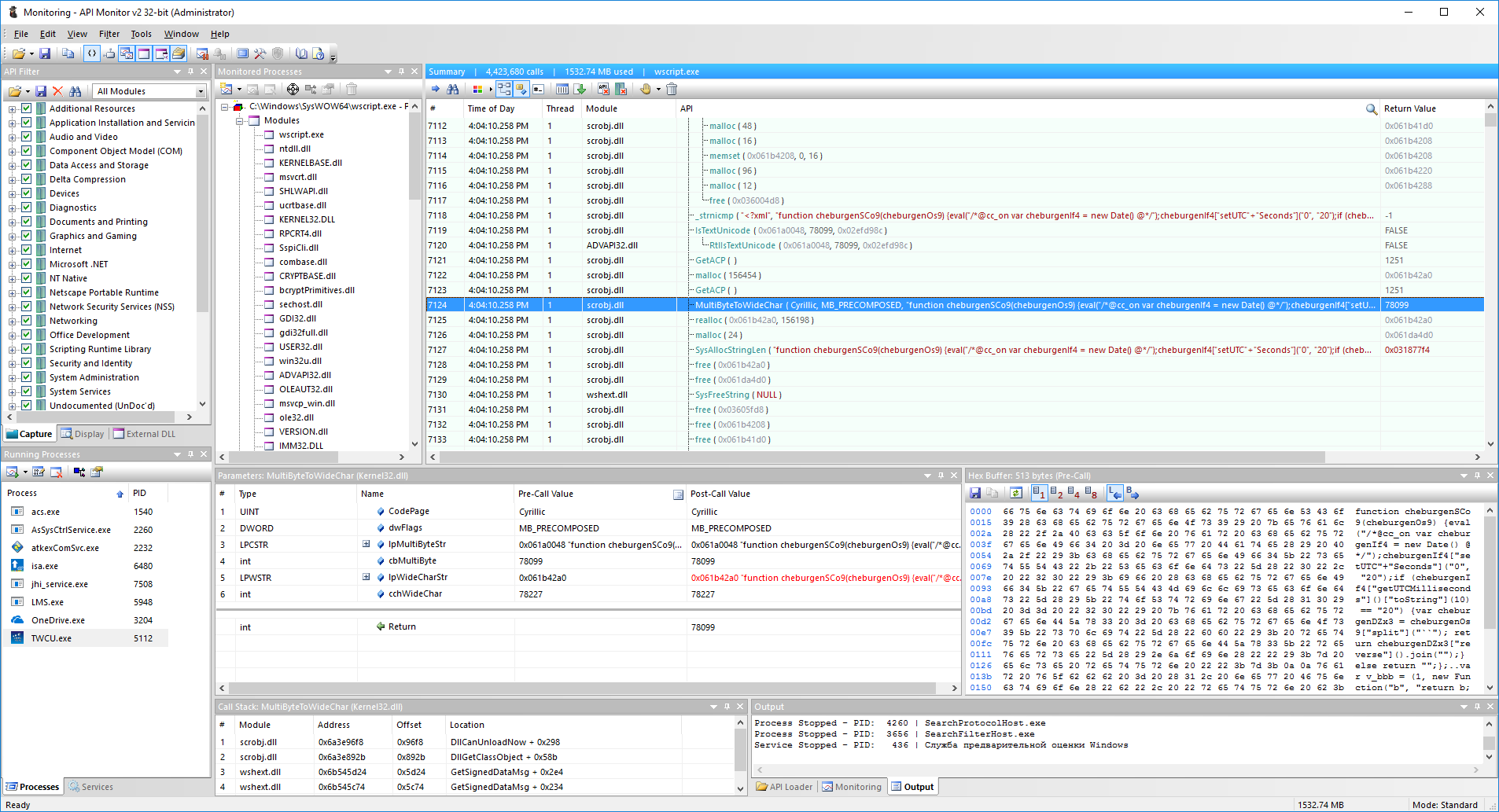
A Locky-hoz hasonlóan a [féregszerű terjesztési technika](https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm%25253aWin32%25252fLocky&ThreatID=-2147420586) miatt az Osiris-t is trójai titkosító vírusként osztályozzák. Képes mindenféle felhasználói közreműködés nélkül terjedni a hálózaton; egyes áldozatok arról számoltak be, hogy a támadás terjedésének megállításához [le kellett kapcsolni a tartományvezérlőt](https://community.spiceworks.com/topic/1951835-decrypt-files-encrypted-by-osiris-variant-of-locky-ransomware?page=2). Az Osiris képes megosztott mappák, a hálózathoz kapcsolódó meghajtók, illetve az adott hálózathoz csatlakozó más gépek ezreit megfertőzni. A kár, amit ennyi, egyazon hálózaton található eszköz elvesztése okoz, bármely vállalkozás számára végzetes lehet.

Az Osiris CRM/Ügyféltámogatási rendszereken (felhő alapúakon is) terjeszthető, szervezeti határokon átívelve is. Az egyik szervezet megfertőzött felhasználója küldhet egy e-mailt egy CRM rendszer e-mail címére; ennek belső parsere elemzi a bejövő e-mailt, és a rosszindulatú csatolmányt egy automatikusan generált jegyre teszi. Az ügyféltámogató szakember megnyitja a jegyet, megnyitja az Excel csatolmányt, és megfertőzi a hálózatot.

**Fertőzés**

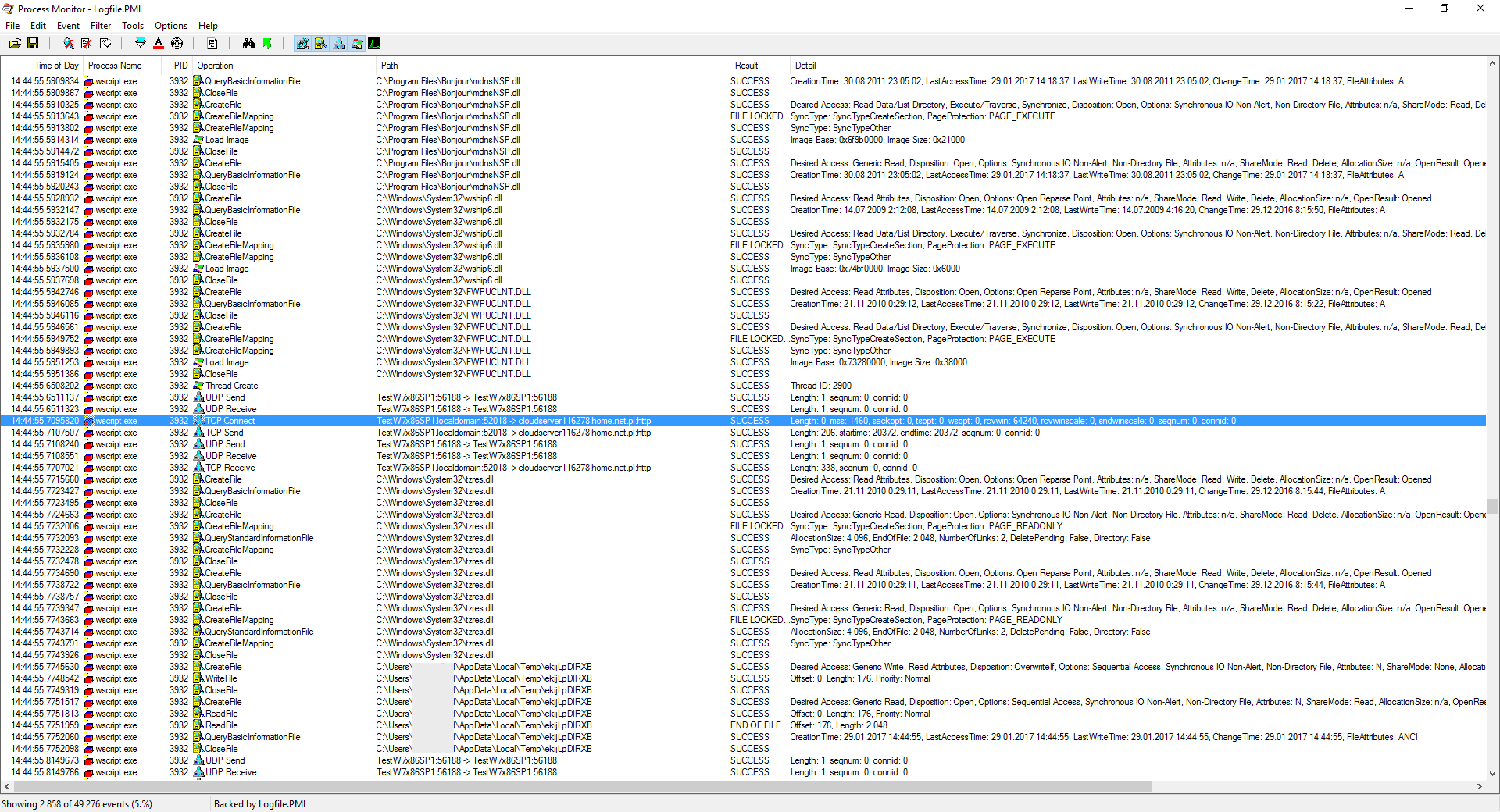
Az Osiris.js dropper a *cheburgen* funkciót használja az *ekijLpDlRXB.zk* zsarolóvírus „payload” letöltéséhez. *(A „cheburgen” egy orosz szóösszetétel, amely az orosz rajzfilmszereplőkre, Cseburaskára és Krokodil Génára utal, vagyis újabb jelzés a zsarolóvírus orosz eredetére.)*

A 2017. január 29-én vizsgált Osiris dropper mérete 71 kB, ami kétszer akkora, mint a 2016 decemberében vett korábbi minták. Ezt jelenleg a Windows Defender sem észleli.



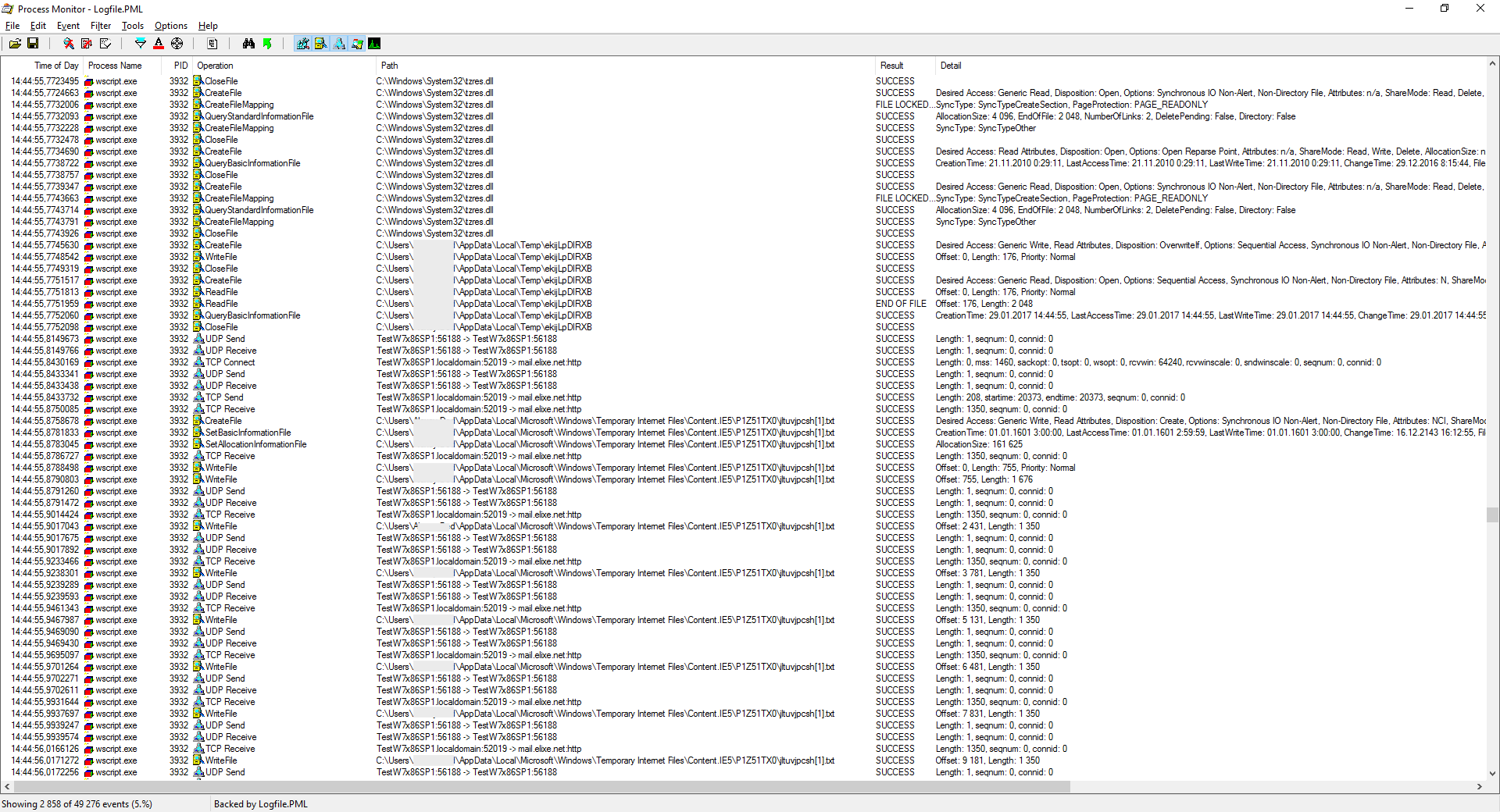
*A cheburgern funkció futtatását bemutató API Monitor képernyőkép.*

A „payload” első letöltési kísérleteire egy lengyel szerverre csatlakozva került sor.



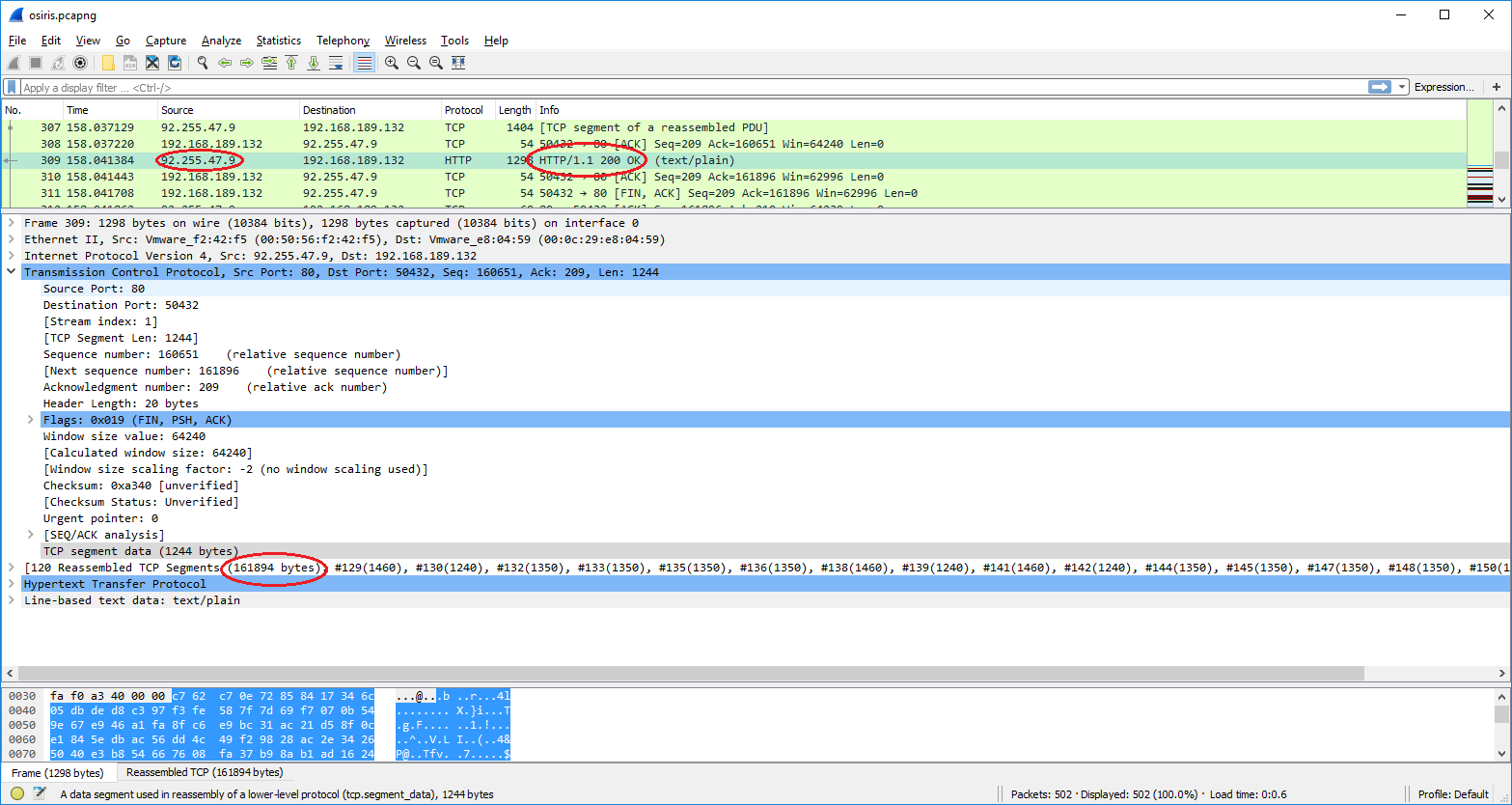
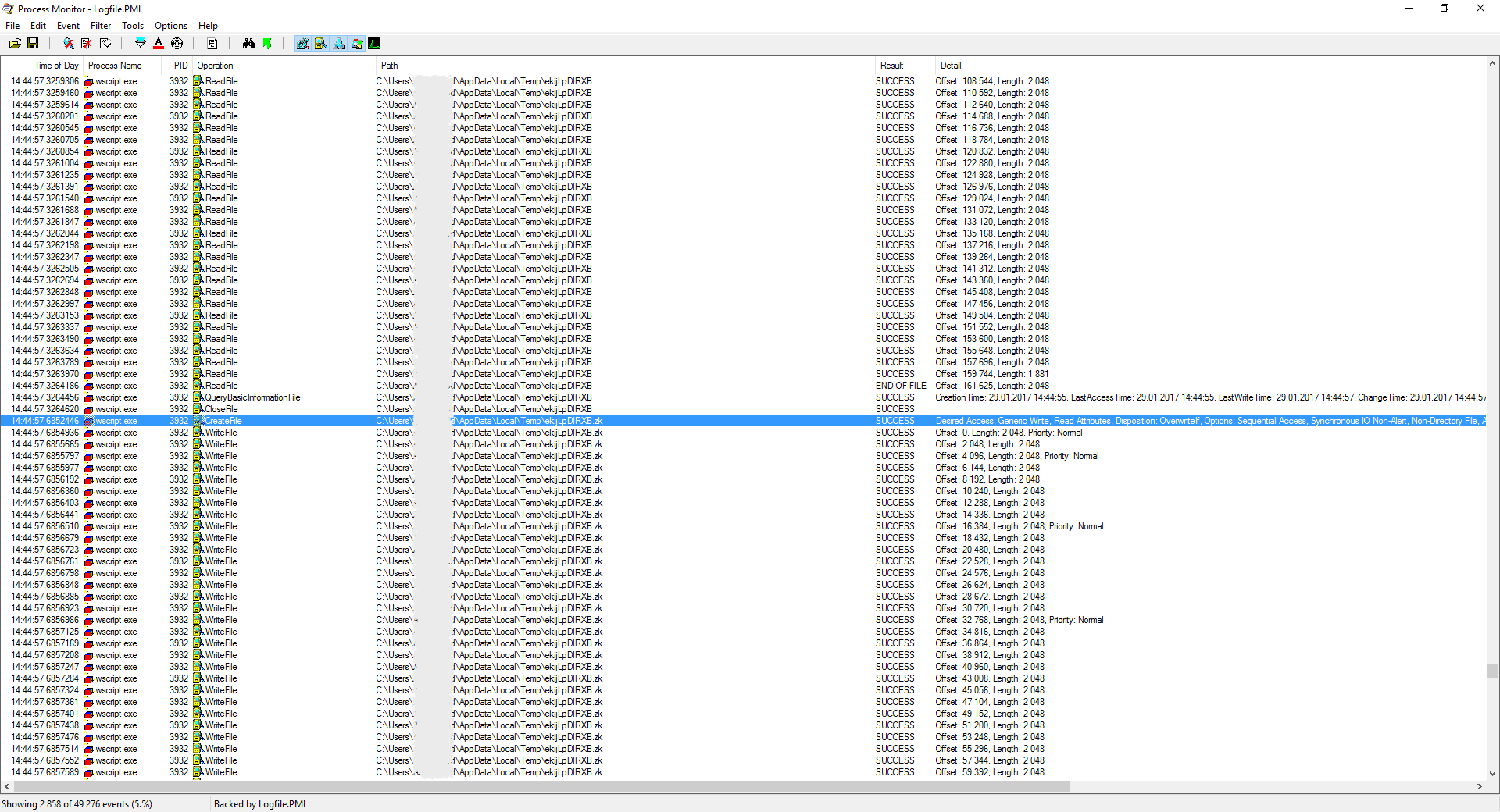
*Process Monitor képernyőkép arról, amint a dropper csatlakozik a home[.]net[.]pl-re*

Később azonban váltott az orosz elixe[.]net szerverre, amelyet jelenleg a legtöbb anti-malware program blokkol.



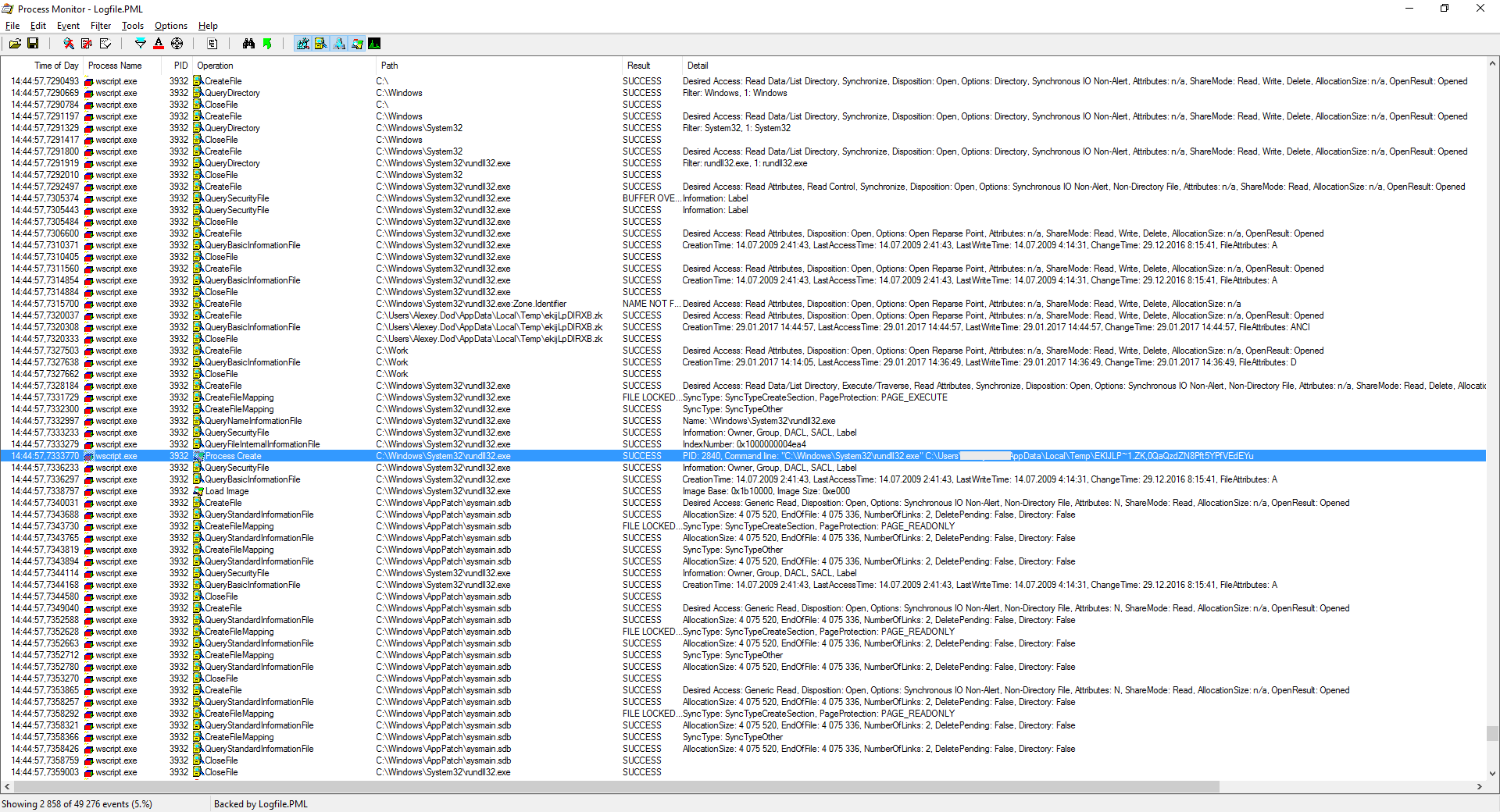
*Process Monitor képernyőkép, amely a rosszindulatú szoftver letöltését mutatja elixe[.]net-ről.*

*Process Monitor képernyőkép, amely az ekijLpDlRXB.zk letöltésének folyamatát mutatja a felhasználó Temp könyvtárába.*



*Wireshark képernyőkép, amely a 161894 bájt méretű letöltött „payload”-ot mutatja. A 92.255.47.9 IP-szám alighanem az Osiris C&C IP-szám készletéhez tartozik.*

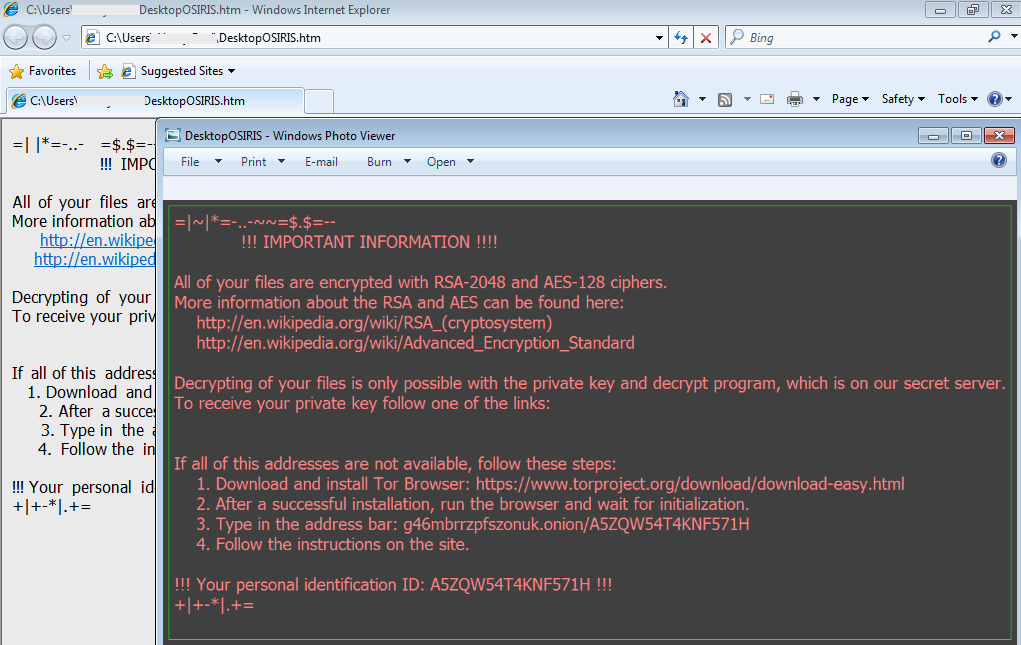
A sikeres letöltést követően az ekijLpDlRXB.zk a rundll32.exe segítségével aktiválódik, a következő parancsra:  
"C:\Windows\System32\rundll32.exe" C:\Users\User.Name\AppData\Local\Temp\EKIJLP~1.ZK,0QaQzdZN8Pft5YPfVEdEYu



*Process Monitor képernyőkép, amely a folyamat runndll32.exe segítségével történő futtatását mutatja be.*

Az aktiválás után az Osiris azonnal elkezdi titkosítani a fájlokat, majd az alapértelmezett böngésző, pl. Firefox segítségével megjeleníti a zsaroló üzenetet:

firefox.exe -osint -url "%USERPROFILE%\DesktopOSIRIS.htm"



*Váltságdíjat követelő Osiris-üzenetek.*

**Virtualizáció észlelése**

Úgy tűnik, hogy a 2016 júliusában bevezetett VM észlelési mechanizmus nem hozta a várt eredményeket. Az Osiris megalkotói vélhetően úgy fejlesztették tovább a logikát, hogy a GetProcessHeap() funkciót GetOEMCP()-ra cserélték, CPU-ciklusok alapján (10 helyett 20) frissítették a virtualizáció észlelésének feltételeit, és növelték az ellenőrzések számát (1-ről 2-re). A VM-észlelés feltételeit is megváltoztatták, tízszeresről háromszorosra csökkentve a virtuális és a fizikai környezetre jellemző futtatási idők közötti különbséget.

A VM-észlelés rendeltetése megakadályozni, hogy biztonsági cégek egy virtuális gépen tesztelhessék a zsarolóvírust. Az algoritmus azonban nem elég hatékony, mivel az Acronis Security Team sikeres teszteket hajtott végre virtuális környezetben. A funkció pszeudokódja alább látható:

**BOOL passNewImprovedVMCheck()**

**{**

**unsigned \_\_int64 tsc1;**

**unsigned \_\_int64 tsc2;**

**unsigned \_\_int64 tsc3;**

**BOOL firstPassResult;**

**BOOL secondPassResult;**

**int i = 0;**

**// Try this 20 times fighting with fluctuations (older Locky variants used 10 times) - the first pass, the older Locky had only 1 pass**

**for (i = 0; i < 20; i++)**

**{**

**tsc1 = \_\_rdtsc();**

**// This function execution should be faster than CloseHandle on the physical machine**

**GetOEMCP();**

**tsc2 = \_\_rdtsc();**

**// This function execution should take more time than GetOEMCP on the physical machine**

**CloseHandle(0);**

**tsc3 = \_\_rdtsc();**

**// Did it take at least 3 times more (was 10 times more in the older Locky variants)**

**// CPU cycles to execute CloseHandle than it took to execute GetOEMCP()?**

**if ( ( LODWORD(tsc3) - LODWORD(tsc2) ) / ( LODWORD(tsc2) - LODWORD(tsc1) ) >= 3)**

**firstPassResult = TRUE;**

**}**

**if (!firstPassResult)**

**{**

**// The consistent small ratio of difference between GetOEMCP and CloseHandle execution times - so we're probably in a VM!**

**return FALSE;**

**}**

**// Do the second pass**

**...**

**if ( ( LODWORD(tsc3) - LODWORD(tsc2) ) / ( LODWORD(tsc2) - LODWORD(tsc1) ) >= 3)**

**secondPassResult = TRUE;**

**}**

**if (!secondPassResult)**

**{**

**// The consistent small ratio of difference between GetOEMCP and CloseHandle execution times - so we're probably in a VM!**

**return FALSE;**

**}**

**return TRUE; }**

## Támadások a biztonsági mentés ellen

Hogy az áldozatok ne állíthassanak helyre fájlokat a biztonsági mentésből a váltságdíj kifizetése nélkül, az Osiris kikapcsolja a Volume Shadow Copy Service-t (VSS). Ez a technológia a Microsoft Windows része, és lehetővé teszi manuális vagy automatikus biztonsági másolatok vagy pillanatfelvételek készítését számítógépes fájlokról vagy kötetekről.

Az Osiris csendes üzemmódban a „vssadmin.exe Delete Shadows /All /Quiet” parancs futtatásával a már létrehozott árnyékmásolatokat is törli.

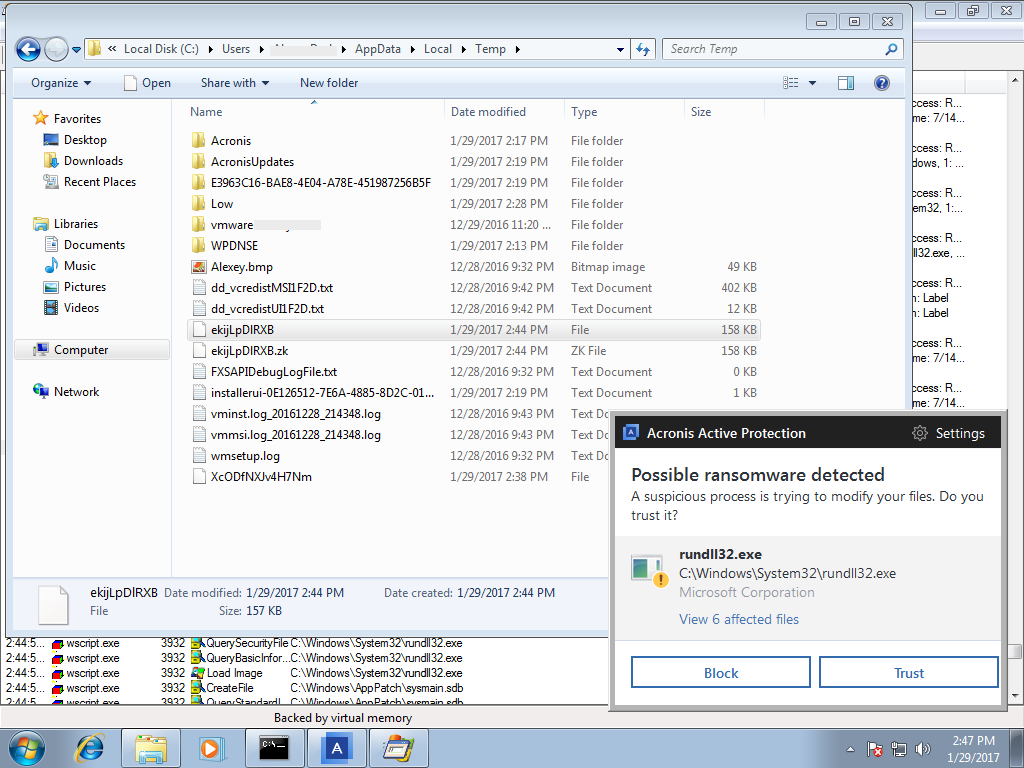
Így a megfertőzött gépen a felhasználók nem tudnak rendszer-helyreállítást végezni az elmentett adatokból.

A Microsoft VSS nem tartalmaz biztonsági intézkedéseket saját maga és a létrehozott árnyékmásolatok védelmére törlés vagy módosítás ellen. Az Acronis ilyen támadásokat jósol a biztonsági mentési megoldások ellen, és saját termékeit önvédelmi technikákkal látta el. Független tesztek bizonyítják, hogy ennek az egyedülálló képességnek köszönhetően az Acronis termékek ellenállnak az olyan támadásoknak, mint az Osiris.

## Hogyan védhetjük meg rendszerünket az Osiris zsarolóvírustól?

Az Osiris fájlok manuális „dekódolása” bonyolult, és csak akkor lehetséges, ha a felhasználók rendelkeznek még nem titkosított biztonsági másolatokkal.

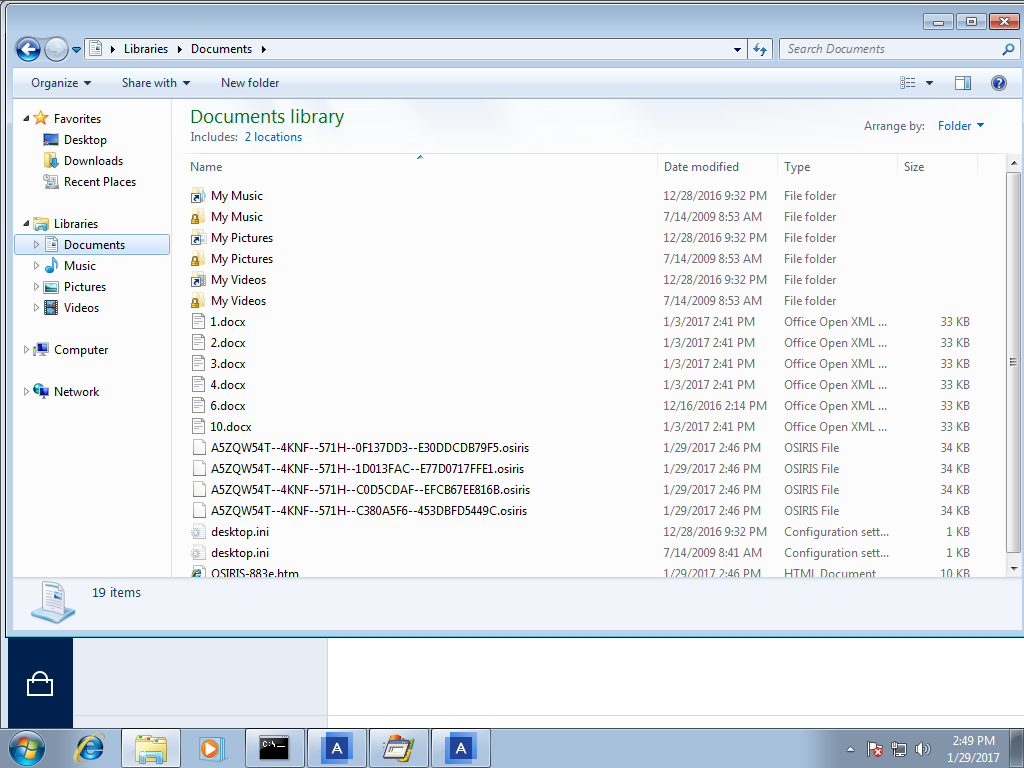
Az Acronis Active Protection™ igazoltan sikeres védelmet nyújt számítógépes rendszerek számára az Osiris zsarolóvírus ellen. Ez az Acronis True Image 2017 New Generation-nél bevezetett innovatív, szabadalmaztatás előtt álló technológia viselkedési heurisztikán alapul, és könnyen érzékeli és leállítja az Osiris rosszindulatú tevékenységét. Lehetővé teszi azt is, hogy a felhasználó azonnal helyreállítson bármilyen érintett fájlt.



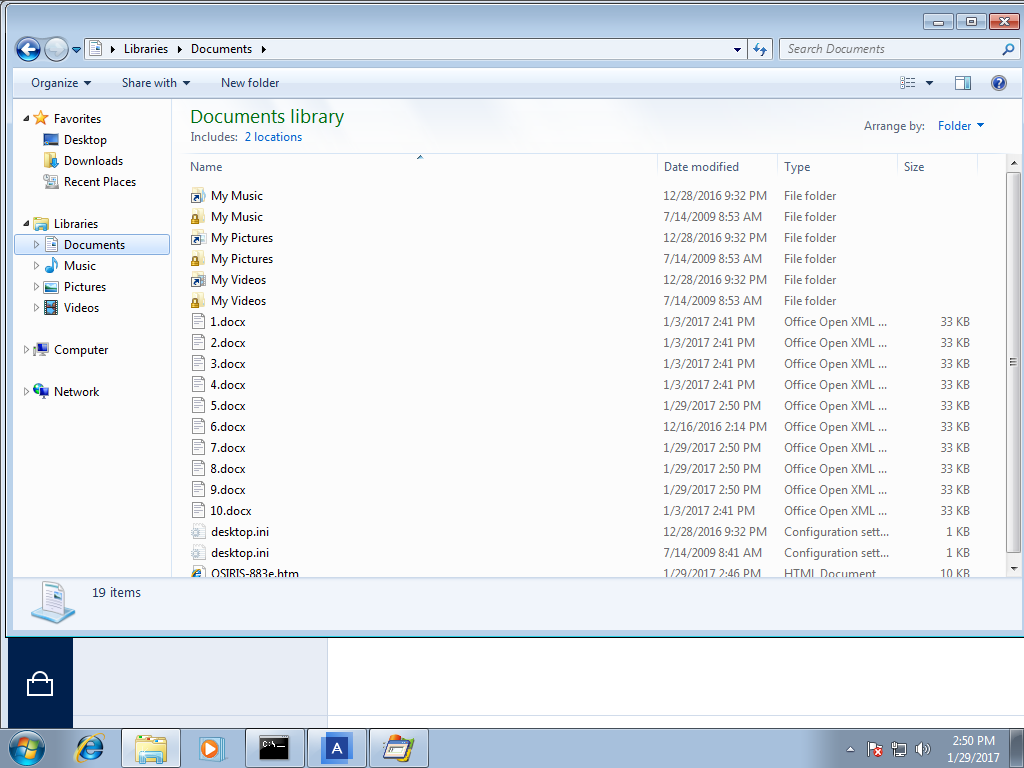
*Osiris zsarolóvírus észlelése egy Acronis True Image 2017 New Generation-t futtató számítógépen, az Acronis Active Protection engedélyezésével.*



*A képernyőkép azt mutatja, hogy a támadást sikerült megállítani, de 6 fájl titkosítása már megtörtént.*



*A .osiris zsarolóvírus által titkosított 4 fájl*



*Valamennyi fájl eredeti állapotában helyreállításra került az Acronis Active Protection™ segítségével, a váltságdíj kifizetése nélkül.*

## Megengedheti magának, hogy elveszítsen 8 évnyi adatot?

Vélhetően az Osiris zsarolóvírus e változata felelős a Texas állambeli Cockrell Hill-i rendőrség ellen intézett támadásért is, amely 8 évnyi fontos bizonyíték elvesztéséhez vezetett.

Nyilvános közleményében a rendőrség elmondta, hogy a rosszindulatú szoftver „egy klónozott e-mail címről érkezett, amely egy, a rendőrség által kiadott e-mail címnek álcázta magát”, és miután bejutott, 4 bitcoin váltságdíjat követelt, amelynek értéke ma 3 600 dollár, illetve a rendőrség megfogalmazásában „csaknem 4 000 dollár”, jelentette a The Register. Az adatok azért vesztek el, mert a rendőrség nem rendelkezett megfelelő biztonsági mentési eljárásokkal.

Más híradások szerint bűnözők zsarolóvírussal támadták meg Ausztriában a Romantik Seehotel Jaegerwirt hotelt az alpesi Turracher Hühe hágónál, amely során feltörték az elektronikus zárrendszert, és vendégek százait zárták be szobáikba – vagy éppen ki szobáikból –, amíg sor nem került a váltságdíj kifizetésére.

Ön megengedheti magának, hogy a zsarolóvírusok következő áldozata legyen?

**Védje meg rendszereit még ma!** Ha szeretné megtudni, erre hogyan van mód, töltse le a következőt: [Acronis Active Protection: Constant data availability in a changing threat landscape.](http://download.acronis.com/pdf/ATI2017NG_whitepaper_active-protection_en-US.pdf)