# Kum Havuzu Tespiti

written by Mert SARICA | 2 December 2019
If you are looking for an English version of this article, please visit here.

8-9 yıl önce yazdığım blog yazılarında (Anti Analiz, Anti Anti-VMWare) zararlı yazılım geliştiren art niyetli kişilerin, zararlı yazılımlarının sanal sistemlerde güvenlik araştırmacıları veya güvenlik sistemleri tarafından analiz edilmesini zorlaştırma, engelleme adına çeşitli yöntemlerden faydalandıklarından bahsetmiştim.

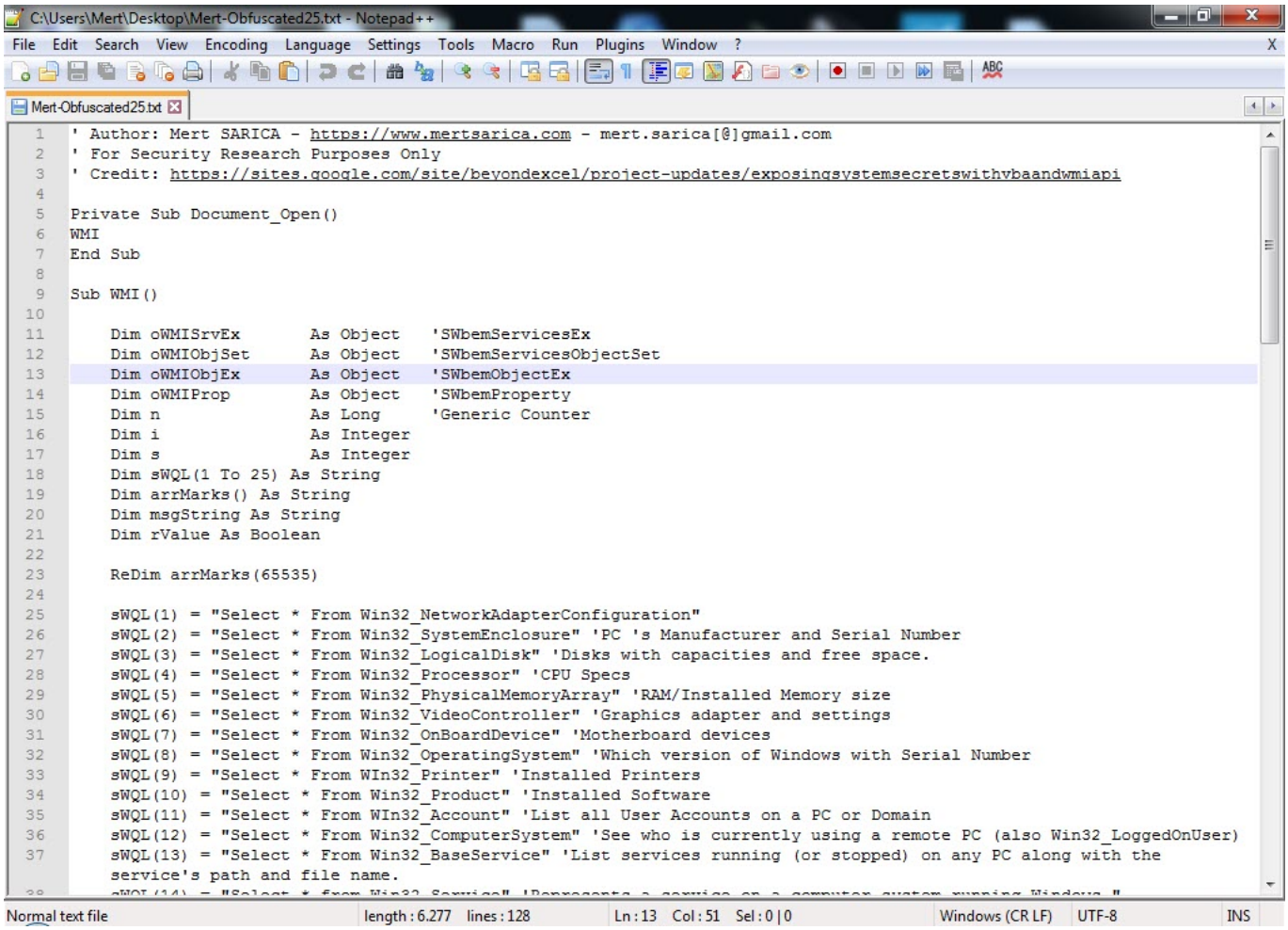
Tabii günümüzde Virtual Desktop Infrastructure (VDI) teknolojilerinin kurumsal ortamlarda son kullanıcılar tarafından yaygın olarak kullanılmaya başlanmasıyla sanal sistemlerin çoğunlukla sunucular veya zararlı yazılım analistleri, güvenlik araştırmacıları tarafından kullanıldığı günler geride kalmaya başladı. Durum böyle olunca da zararlı yazılım geliştiricilerinden kırmızı takım (red team) çalışması gerçekleştiren etik hackerlara kadar hedef sistemleri kendi araçları ile uzaktan yönetmek ancak yakalanmak istemeyenlerin ortak kaygısı, sanal sistemlerde çalışabilen fakat analiz sisteminde çalışmayan araçlar tasarlamak ve geliştirmek olmaya başladı. Gerçekçi bir yaklaşımla analiz sisteminde çalışmayan bir aracın geliştirilmesinin mümkün olamayacağını bilen zararlı yazılım geliştiricileri, yakalandıklarını anlamak ve operasyonlarını durdurmak için VirusTotal üzerinde belli zaman aralıklarında geliştirdikleri zararlı yazılımlarının hash değerlerini aratmaktadırlar. Benzer şekilde mavi takım tarafından yakalanabileceği ihtimalini göz ardı etmeyen kırmızı takım çalışanları ise operasyonlarının sürdürülebilirliğini sağlama adına RedELK gibi projelerden faydalanmaktadırlar.

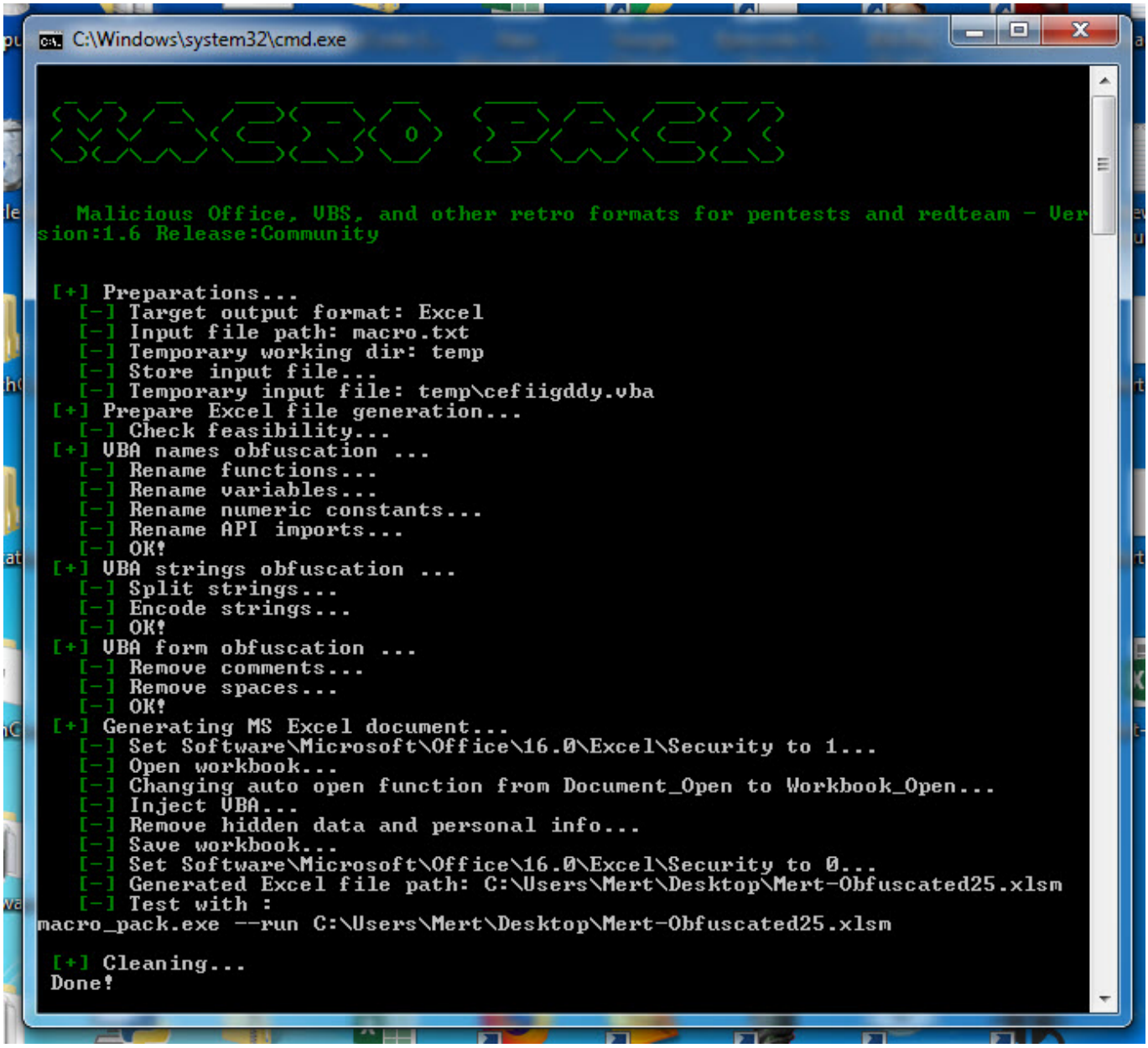
Zararlı olduğundan şüphe edilen dosyaların son kullanıcılar, güvenlik uzmanları tarafından VirusTotal, Any.Run, Hybrid Analysis, Lastline Analyst, VMRay Analyzer vb. kum havuzu sistemlerine yüklendiğini bildiğim için çok güvendiğimiz bu kum havuzu sistemlerini tespit etmenin pratikte ne kadar kolay veya zor olduğunu araştırmaya ve sizlerle paylaşmaya karar verdim.

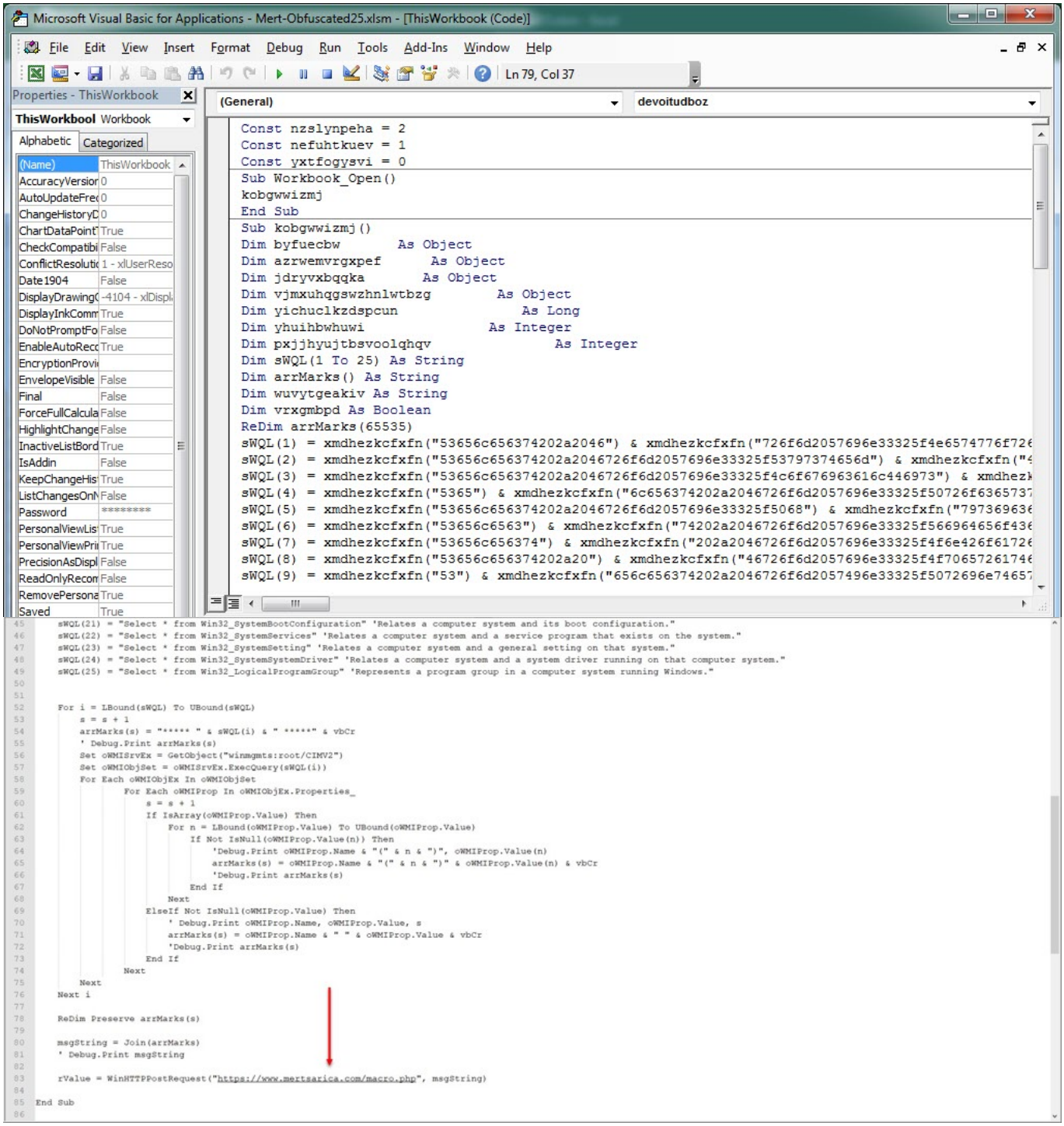
Bunun için ilk olarak kum havuzu sistemleri ile ilgili bilgi toplamam (keşif) gerekiyordu. Kum havuza sistemine yüklenen bir yazılım, dinamik analiz esnasında hedef bir sistem (c&c) ile haberleşmeye geçtiğinde kum havuzu sistemi tarafından izlenmekte ve kayıt altına alınmakta kısaca bu sistemler üzerinde internetteki bağlantısına izin verilmektedir. Ben de bu fırsattan

istifade ederek hedef işletim sistemi ile ilgili bilgi toplayan bir Microsoft Office makrosu hazırlamaya karar verdim. Makro ile bu işi yapmanın en kolay yolu özellikle hedeflenmiş saldırılarda (APT) yanal hareket (lateral movement) amacıyla kullanılan Windows Management Instrumentation (WMI)'dan faydalanmaktı. WMI ile ilgili olarak Microsoft'un sitesinde ufak bir araştırma yaptığınızda (Win32 Provider) hedef işletim sistemi ile ilgili çok ama çok sayıda bilgi toplayabildiğinizi görebilirsiniz.

Dünyayı yeniden keşfetmeme adına Google'da ufak bir arama yaptığımda VBA ile WMI üzerinden bilgi toplamaya yarayan basit bir betik ile karşılaştım. Bu betik dosyasına Microsoft'un sayfasında işletim sistemine yönelik olan 25 adet sınıfı ekledikten sonra bu bilgileri https://www.mertsarica.com/macro.php adresine göndermesini sağladım. Antivirüs yazılımları tarafından kolayca tespit edilememesi adına da macro_pack aracı ile makroyu gizledim. (obfuscation)



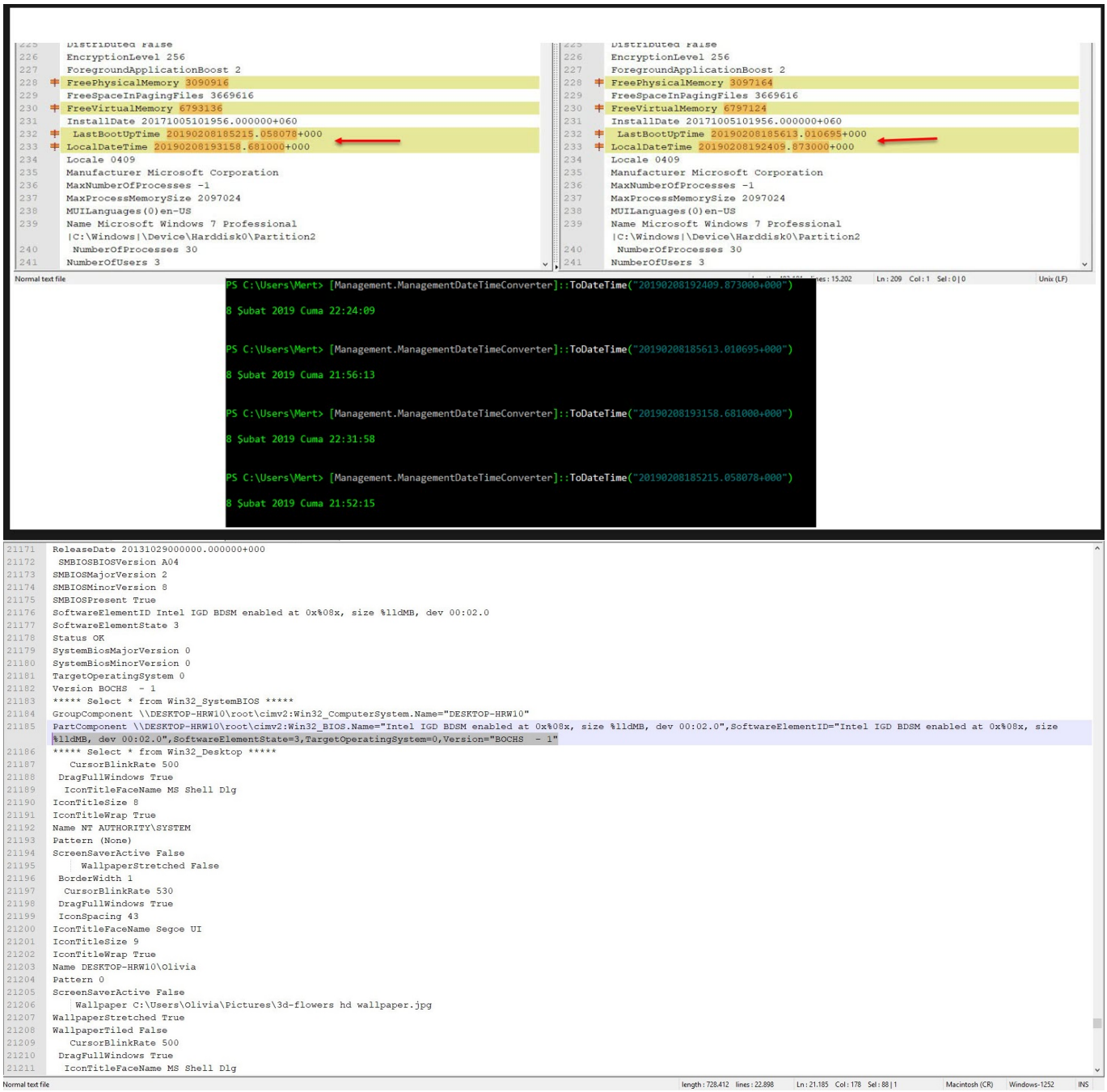

C:\Windows\system32\cmd.exe
Malicious Office, VBS, and other retro formats for pentests and redteam - Version:1.6 Release:Community
[+] Preparations...
[-] Target output format: Excel
[-] Input file path: macro.txt
[-] Temporary working dir: temp
[-] Store input file...
[-] Temporary input file: temp\cefiigddy.vba
[+] Prepare Excel file generation...
[-] Check feasibility...
[+] VBA names obfuscation ...
[-] Rename functions...
[-] Rename variables...
[-] Rename numeric constants...
[-] Rename API imports...
[-] OK!
[+] VBA strings obfuscation ...
[-] Split strings...
[-] Encode strings...
[-] OK!
[+] VBA form obfuscation ...
[-] Remove comments...
[-] Remove spaces...
[-] OK!
[+] Generating MS Excel document...
[-] Set Software\Microsoft\Office\16.0\Excel\Security to 1...
[-] Open workbook...
[-] Changing auto open function from Document_Open to Workbook_Open...
[-] Inject VBA...
[-] Remove hidden data and personal info...
[-] Save workbook...
[-] Set Software\Microsoft\Office\16.0\Excel\Security to 0...
[-] Generated Excel file path: C:\Users\Mert\Desktop\Mert-Obfuscated25.xlsm
[-] Test with :
macro_pack.exe --run C:\Users\Mert\Desktop\Mert-Obfuscated25.xlsm
[+] Cleaning...
Done!




Mert-Obfuscated25.xlsm dosyasını Any.Run ve VirusTotal'a yükledikten kısa bir süre sonra https://www.mertsarica.com/macro.php dosyasına istekler geldiğini gördüm. Gelen isteklere baktığımda kum havuzu analizi yapan sistemlerle ilgili önümde incelenmesi gereken epey bir bilgi olduğunu gördüm. :)

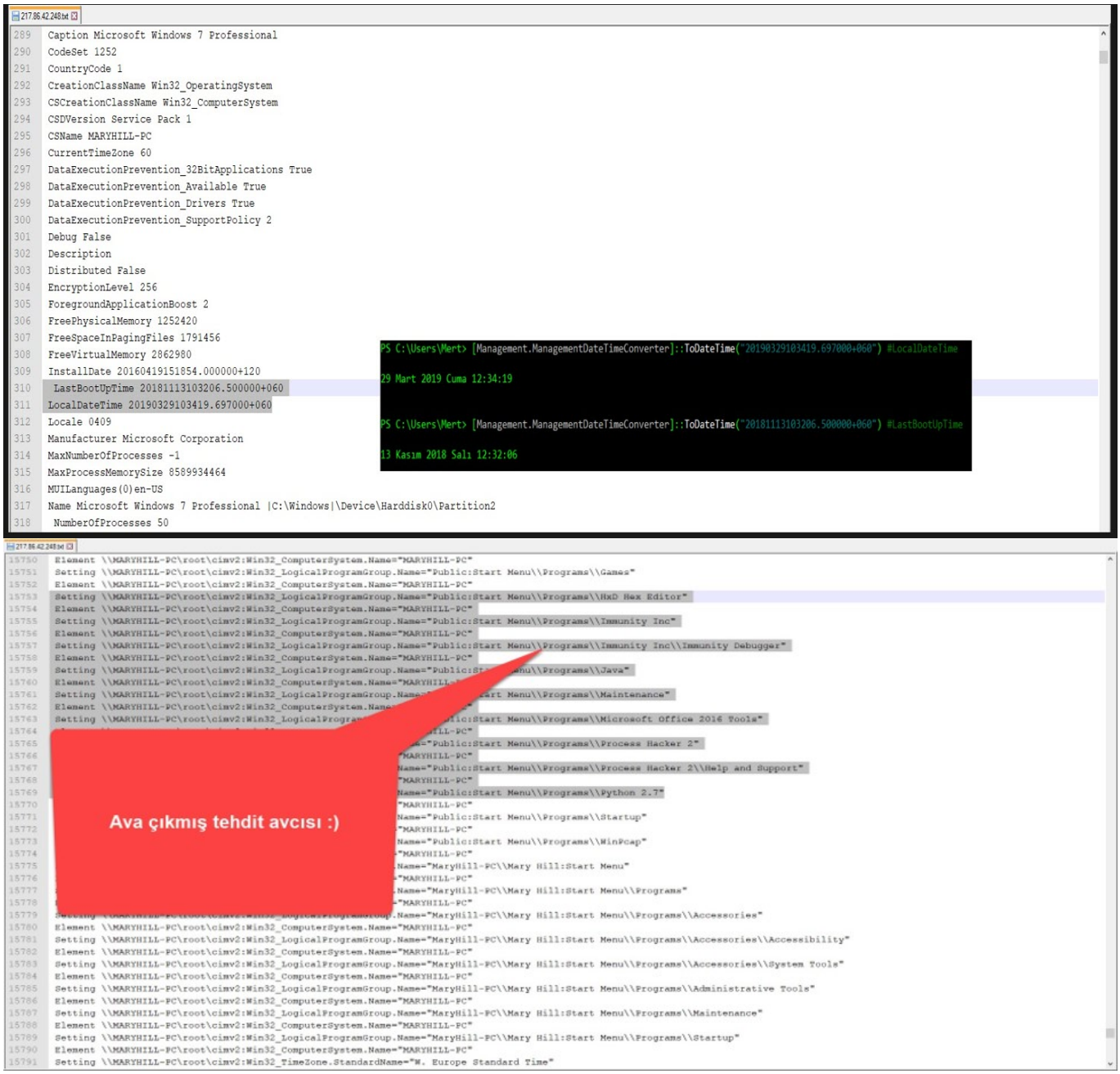
Bu bilgilere bakarken ilk olarak dikkatimi Select * From Win32_OperatingSystem WMI isteğinin çıktısında yer alan LastBootUpTime değeri çekti. Bu değer, işletim sisteminin en son hangi tarih ve saatte başlatıldığını belirtiyordu. Kum havuzu analizi yapan sistemler zararlı yazılımları analiz etmeden önce işletim sistemini sıfırdan, temiz hali ile

başlatmaktadırlar dolayısıyla analizin gerçekleştirildiği işletim sisteminin yeniden başlatılma tarihi (LastBootUpTime) ile analiz tarihi (LocalDateTime) arasında maksimum 30 dakika gibi bir zaman farkı oluşmaktadır. Bu bilgiden de yola çıkarak yazılımın kum havuzunda analiz edildiğini varsaymak mümkümkün olabilmektedir.

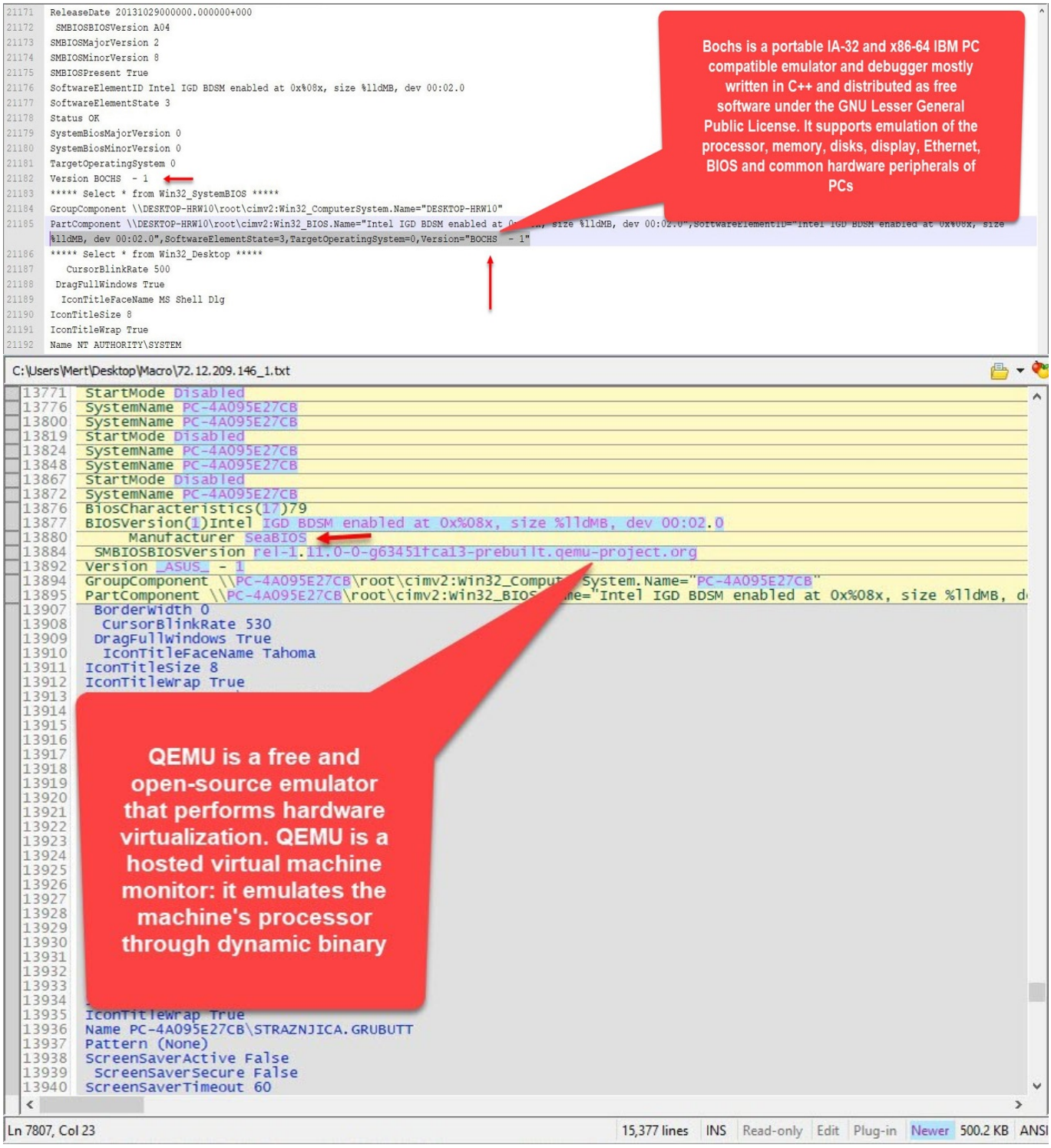



Topladığım bilgilere göz atmaya devam ettiğimde LastBootUpTime ile LocalDateTime arasında 4 ay fark olduğunu fark ettiğim bir çıktı ile karşılaştım. 4 ay boyunca yeniden başlatılmayan bir son kullanıcı sistemi (Windows 7) oldukça şüphe çektiği için bu bilgileri yakından incelemeye başladım. Bilindiği üzere çoğu güvenlik araştırmacısının, zararlı yazılım analistinin hali hazırda izole, sanal bir analiz sistemi bulunmaktadır. Bu

analiz sistemi zaman kaybetmeme adına her defasında yeniden başlatılmak yerine anlık görüntüden (snapshot) döndürülmektedir. Anlık görüntüden döndürülen bir işletim sisteminin de LastBootUpTime günler geçtikçe geride kalmakta ve bir zararlı yazılım analiz edildiğinde LocalDateTime ile arasındaki zaman farkı kimi zaman ayları bulabilmektedir. Bu bilginin ışığında bir de şüphelendiğim bu çıktının Windows işletim sistemindeki program gruplarına Win32_LogicalProgramGroup dair bilgileri topladığı WMI bölümüne baktığımda bu defa güvenlik araştırmacıları, zararlı yazılım analistleri tarafından sıklıkla kullanılan Immunity Debugger, Process Hacker gibi araçların sistem üzerinde yüklü olduğunu gördüm. Bu da bana Office dosyamın bir tehdit avcısı tarafından analiz edildiği bilgisini sağlamış oldu. :)



Son olarak bir de dikkatimi Select * from Win32_SystemBIOS WMI isteğinin çıktısı çekti. Kum havuzlarından gelen bilgilere baktığımda bir tanesinin BOCHS öykünücüsü (emulator) üzerinde bir diğerinin ise QEMU öykünücüsü üzerinde çalıştığını dolayısıyla bu iki sistemin de kum havuzu sistemine ait olduğunu anlamış oldum.




Ekim ayına kadar geçen zaman zarfında macro.php dosyasına istekte bulunan ip adreslerine baktığımda bunların da kuvvetle muhtemel VMRay, Lastline, Any.RUN, VirusTotal'a ait kum havuzu sistemlerine ve bir tehdit avcısına ait

olduğunu söyleyebilirim.

| IP | Domain | Country | Region | City | ISP | ASN | NS |
|---|---|---|---|---|---|---|---|
| 104.215.89.177 | | United States | Texas | San Antonio | Microsoft Corporation | 8075 | |
| 13.80.140.46 | | Netherlands | North Holland | Amsterdam | Microsoft Corporation | 8075 | |
| 188.99.240.204 | dslb-188-099-240-204.188.099.pools.vodafone-ip.de | Germany | Baden-WÃ¼rttemberg Region | Bodman-Ludwigshafen | Vodafone GmbH | 3209 | |
| 217.86.42.248 | pD9562AF8.dip0.t-ipconnect.de | Germany | Baden-WÃ¼rttemberg Region | Tettnang Castle | Deutsche Telekom AG | 3320 | |
| 64.233.172.230 | google-proxy-64-233-172-230.google.com | United States | | | Google LLC | 15169 | |
| 66.102.6.213 | google-proxy-66-102-6-213.google.com | United States | | | Google LLC | 15169 | |
| 66.249.88.41 | google-proxy-66-249-88-41.google.com | United States | California | Mountain View | Google LLC | 15169 | |
| 66.249.88.60 | google-proxy-66-249-88-60.google.com | United States | California | Mountain View | Google LLC | 15169 | |
| 71.59.36.230 | c-71-59-36-230.hsd1.ga.comcast.net | United States | Georgia | Atlanta | Comcast Cable Communications, LLC | 7922 | |
| 72.12.209.146 | | United States | Indiana | Lafayette | Wintek Corporation | 11114 | |
| 85.203.44.80 | | Netherlands | North Holland | Amsterdam | NForce Entertainment B.V. | 43350 | |
| 95.222.167.189 | ip-95-222-167-189.hsi15.unitymediagroup.de | Germany | North Rhine-Westphalia | Bochum | Liberty Global B.V. | 6830 | |

Sonuca gelecek olursam, geliştirilen bir yazılımın, kodun WMI üzerinden elde ettiği bilgiler sayesinde kum havuzu sistemi üzerinde çalıştığını anlaması pratikte zor görünmüyor dolayısıyla hem bu bilgilerden hem de kum havuzu sistemlerine ait olan ip adreslerinden, ip bloklarından faydalanan art niyetli bir kişinin veya bir kırmızı takım üyesinin kum havuzu analizini atlatmasının mümkün olabileceği asla unutulmamalıdır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: 22 Kasım tarihinde düzenlenen NOPcon Uluslararası Hacker Konferansı'nda bu konuyu değindiğim Kum Havuzu Tespiti başlıklı sunum dosyamı dileyenleriniz buradan indirebilirler.