NUKESPED

TEKNİK ANALİZİ

İÇİNDEKİLER

GİRİŞ

Lazarus Apt grubuna ait NukeSped zararlı yazılımı, bir uzaktan erişim Truva atı olan (RAT-Remote Access Trojan) bu kötü yazılım örnekleri , 32 bit sistemler için derlendiği için birden fazla özelliği paylaştığını ortaya koymaktadır. Ayrıca, analizleri engellemek için şifreli dizeler içermektedirler. Kötü amaçlı yazılım, işlevleri dinamik olarak çözmektedir. Ayrıca, içe aktarma tablosunun kısa olduğu ve az sayıda ortak DLL ve işlevi içe aktardığı bulunmaktadır.

Birçok Kuzey Kore hacker grubu tarafından yazılan ve bu gruplardan en bilineni olan Lazarus'a kod kullanımıyla birlikte bağladılar ve bu bağlantıyı güçlendirdiler. Kötü amaçlı yazılımın temel işlevi, saldırganlara virüslü ana bilgisayarın uzaktan yönetimine izin vermektir. Sistem içerisinde analizi zorlaştırırken her API ismini şifrelemekte olup bunları API hammering yöntemiyle hafızasını doldururken Sandboxlarda analizini engellemektedir.

Dosya İsmi	n5JNGFT14Q.exe
MD5	fdc66cdabd46bc3b26aba4e59943726b
SHA1	c341002cc5f9214cc8fd71e633efef673267d1fd
SHA256	5c2f339362d0cd8e5a8e3105c9c56971087bea2701ea3b7324771b0ea2c26c6c
İlk Görüldüğü Tarih	20.06.2021 10:36:59 UTC

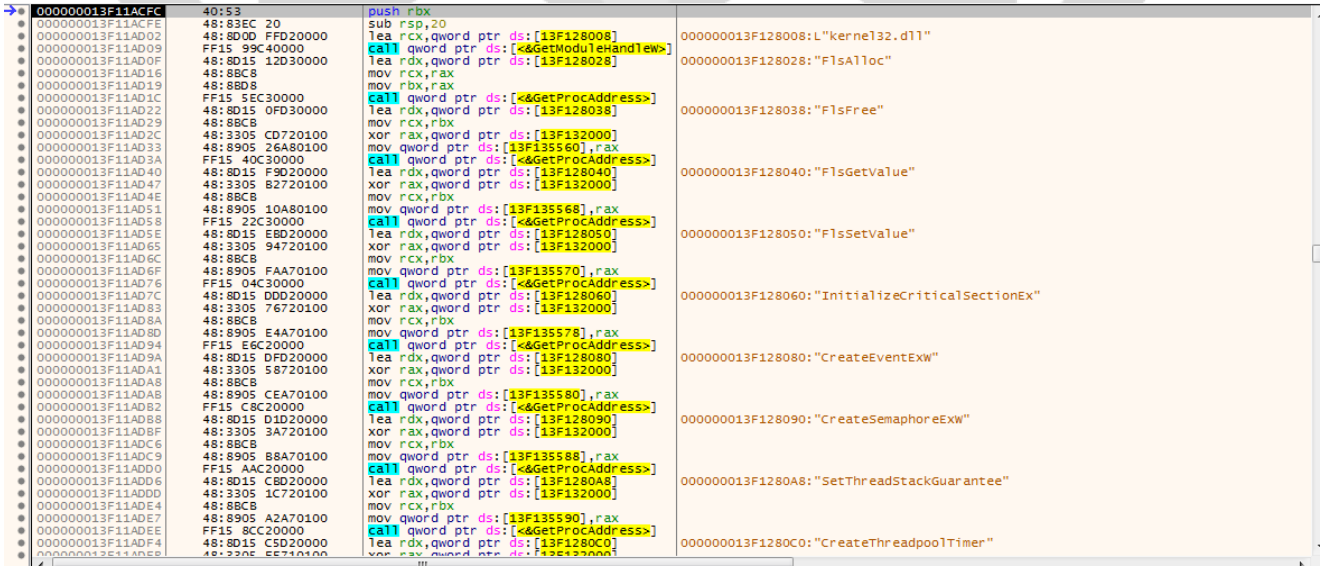
Yüklediği DLL'ler

Zararlı yazılım öncelikle aşağıdaki dll'leri sisteme yüklemekte. Gerekli yüklemeyi yaptıktan sonra bütün API'ları kontrol edip gerekli API'ları encrypt işlemi yaparak kendi hafızasına yazmaktadır.

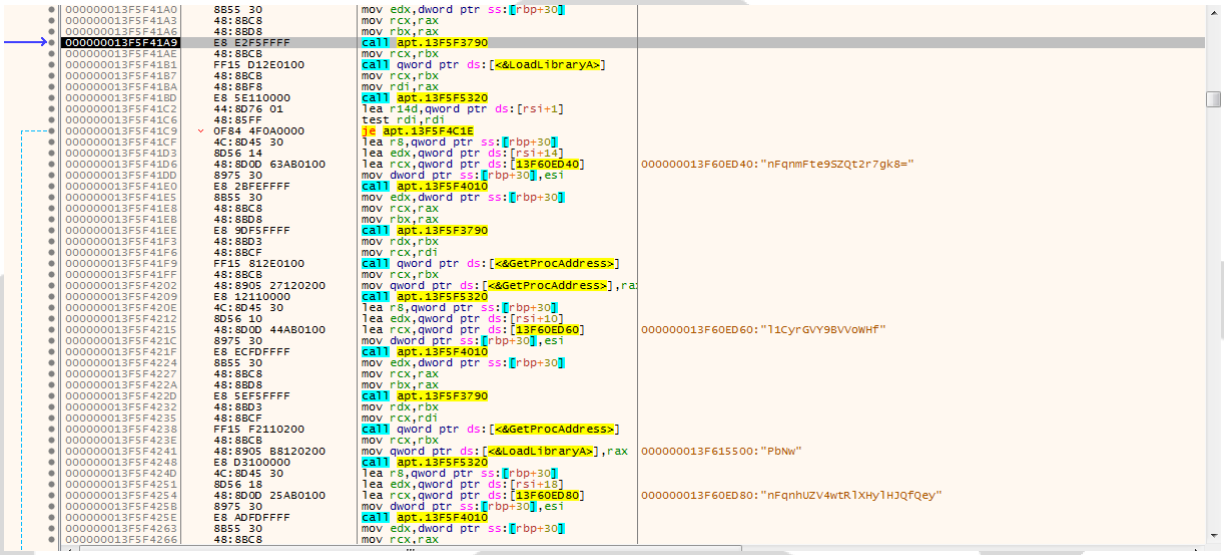
user32.dll	kernel32.dll	ntdll.dll
winnsi.dll	iphlpapi.dll	kernelbase.dll
lpk.dll	gdi32.dll	rpcrt4.dll
msctf.dll	ws2_32.dll	usp10.dll
imm32.dll	nsi.dll	mscvrt.dll

API Obfuscation

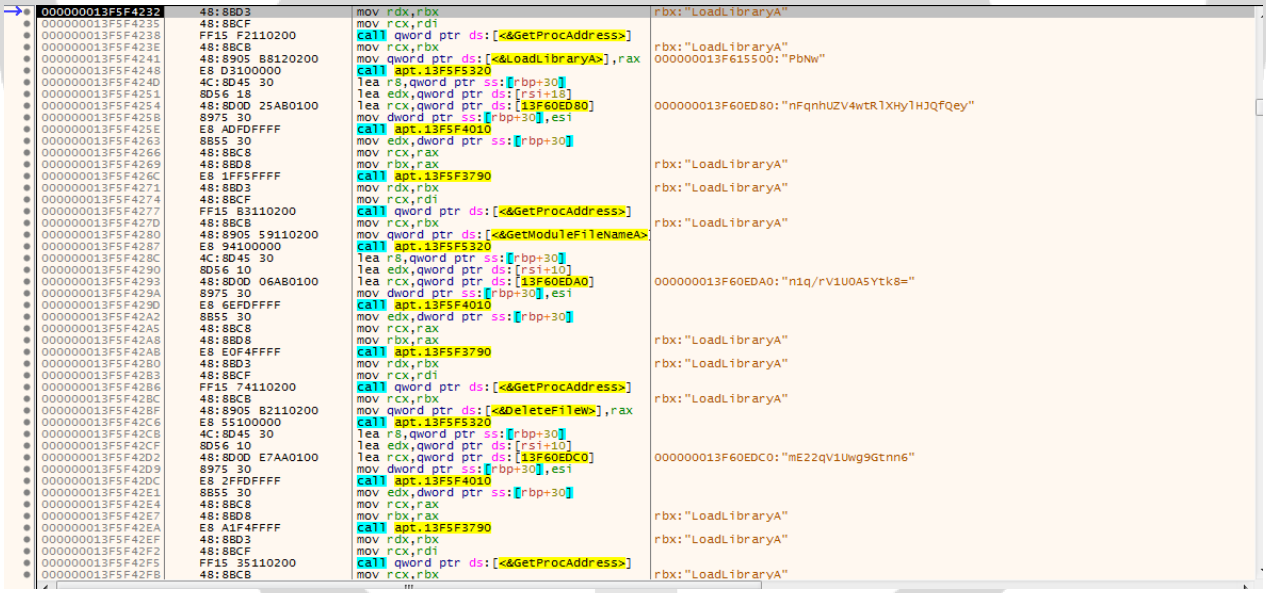
Zararlı yazılım GetModuleHandleW API ile belirtilen modülde handle alıp içerisinden API çağırmakta olup API'ları kontrol etmektedir. Ardından GetProcAddress yardımıyla API isimlerini hafızaya yazmaktadır.



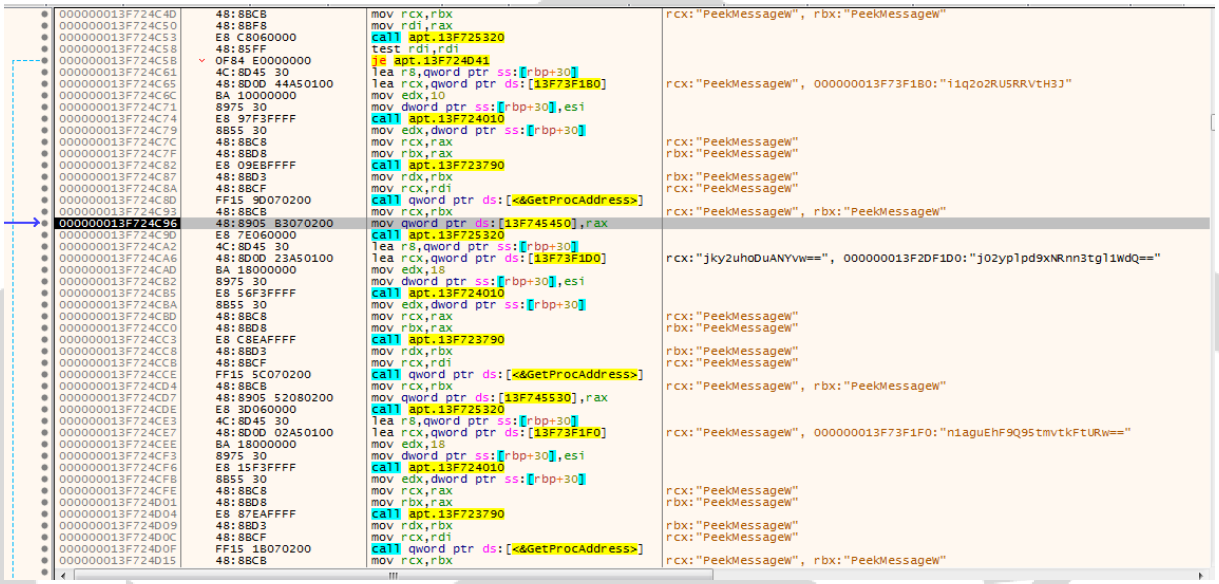
API Obfuscation



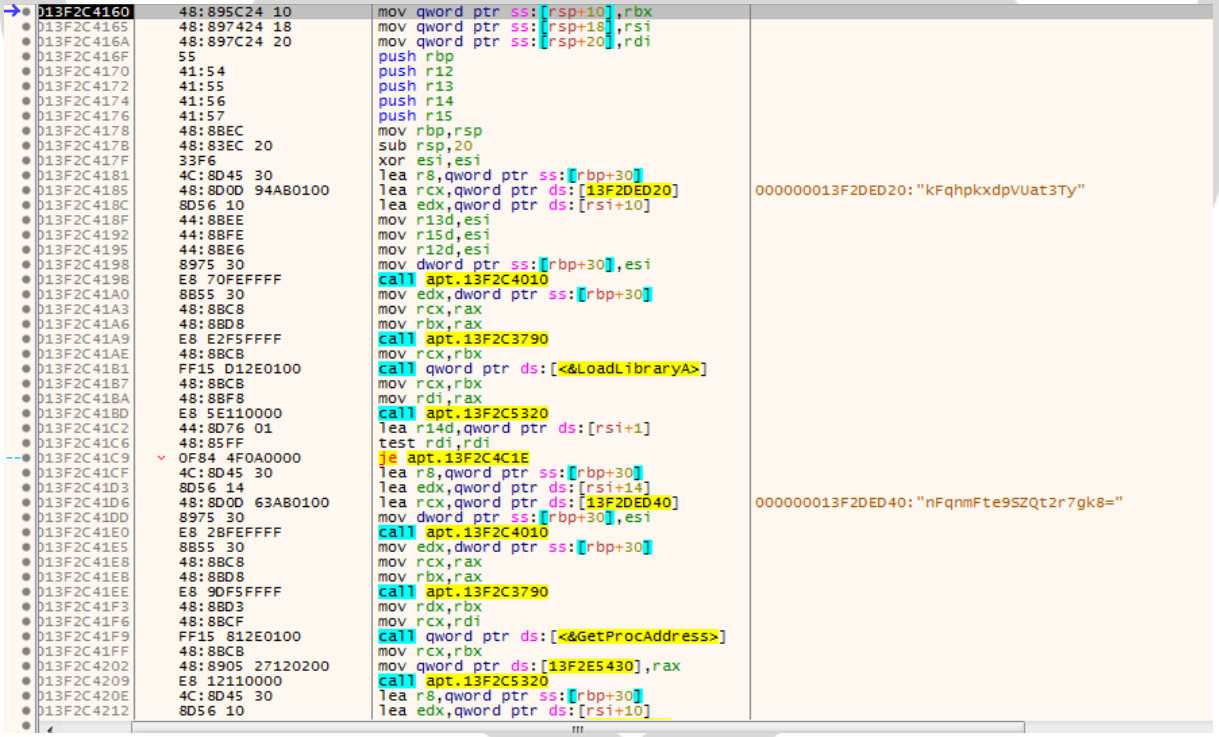
Tüm API'ları şifreleyip eşleşen API'ları tek tek çağırmaktadır. Zararlı yazılım GetProcAddress ile çağırdığı API'ları kendi hafızasına yüklemektedir.



API Obfuscation

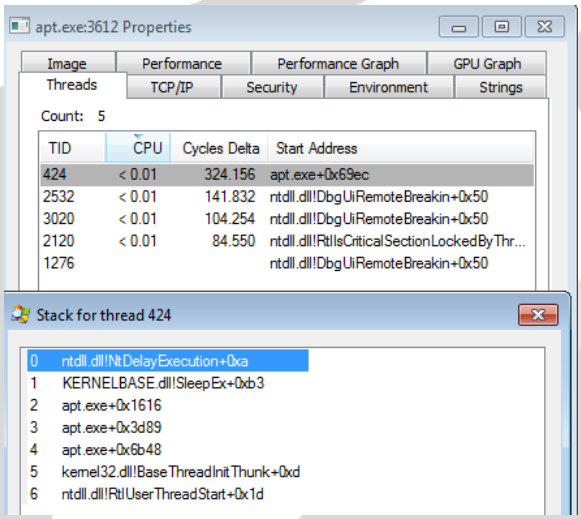


Şifrelediği API'ları hafızadan çağırıp kontrol ettikten sonra çözümleme işlemi yaparak tekrardan hafızasındaki listeyle karşılaştırıp. Eğer kontrol edilen API doğru ise çözümlediği API'ları GetProcAddress API ile kendi hafızasına yüklemektedir.

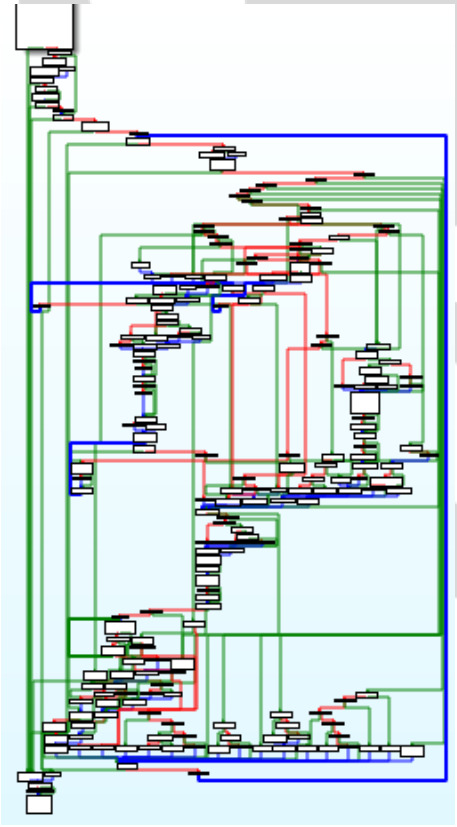


API Hammering

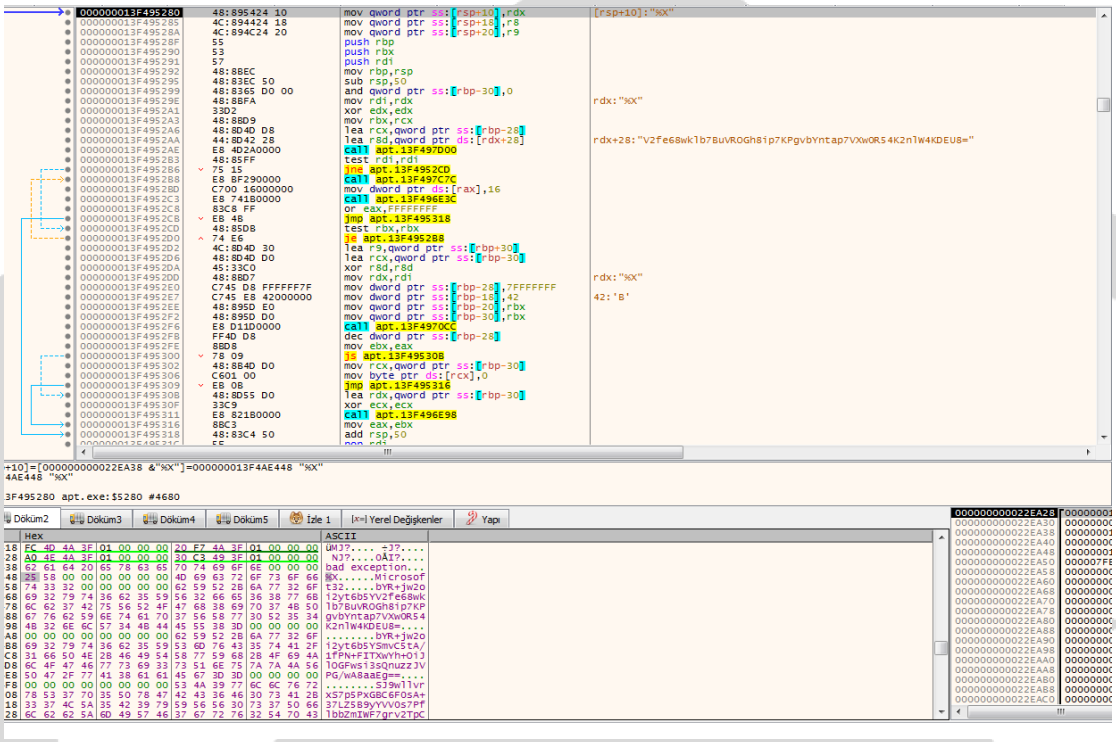
API hammering yöntemiyle birlikte zararlı yazılım kendisini oldukça fazla döngüye sokmaktadır ve ardından alanı çok fazla sayıda gereksiz bilgi ile doldurup sistemi yavaşlatmakta ve çağrı sürecini geciktirmektedir. Bu yöntem sayesinde Sandboxlarda zararlı kod analizi yaptırmamaktadır. Ve bu aşırı yüklenme ise sistem de DelayExecution hatası vermektedir.



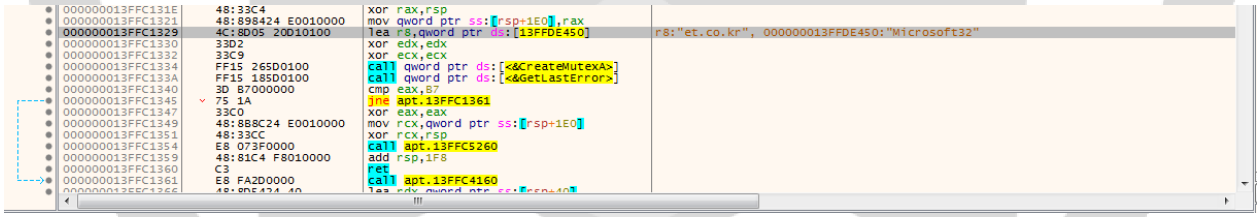
Bu zararlı yazılımda verilebilecek belli başlı API hammering kullanılan API'lar: GetProcAddress, LoadLibraryA, GetModuleHandleW.
Bu API'ları kullanarak sistem üzerinde yoğunluk ve gecikme oluşturup Sandboxlarda bu zararlı kodun çalışmasını engellemektedir.



Mutex Oluşturma

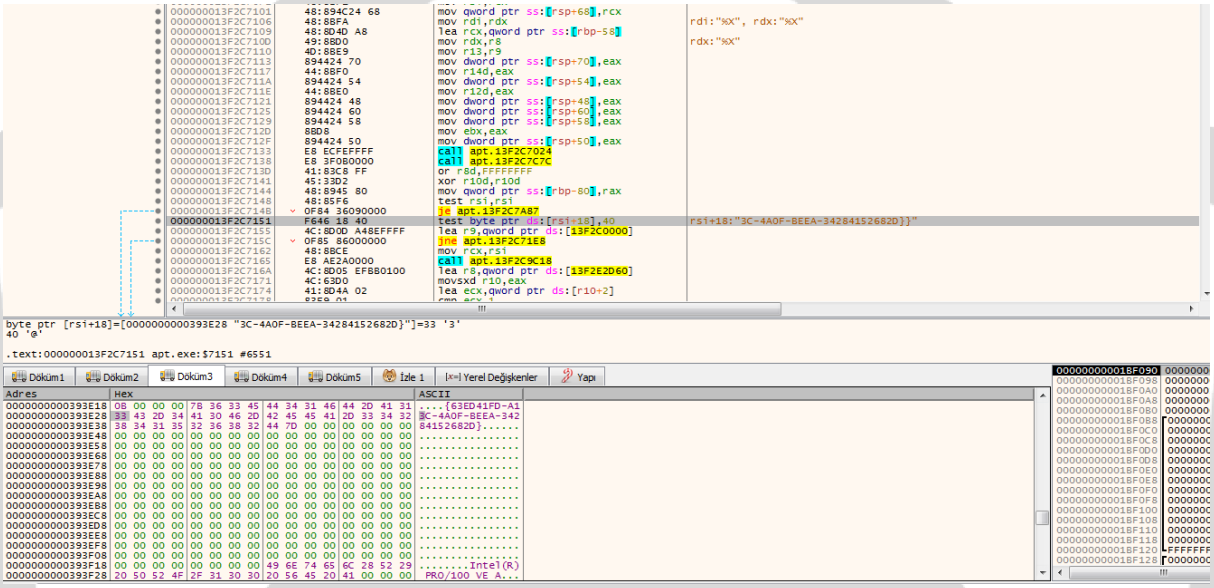


Zararlı yazılım Microsoft32 adı altında bir adet mutex oluşturmakta ve bu mutex bilgisini şifreli şekilde hafızaya yazmaktadır.

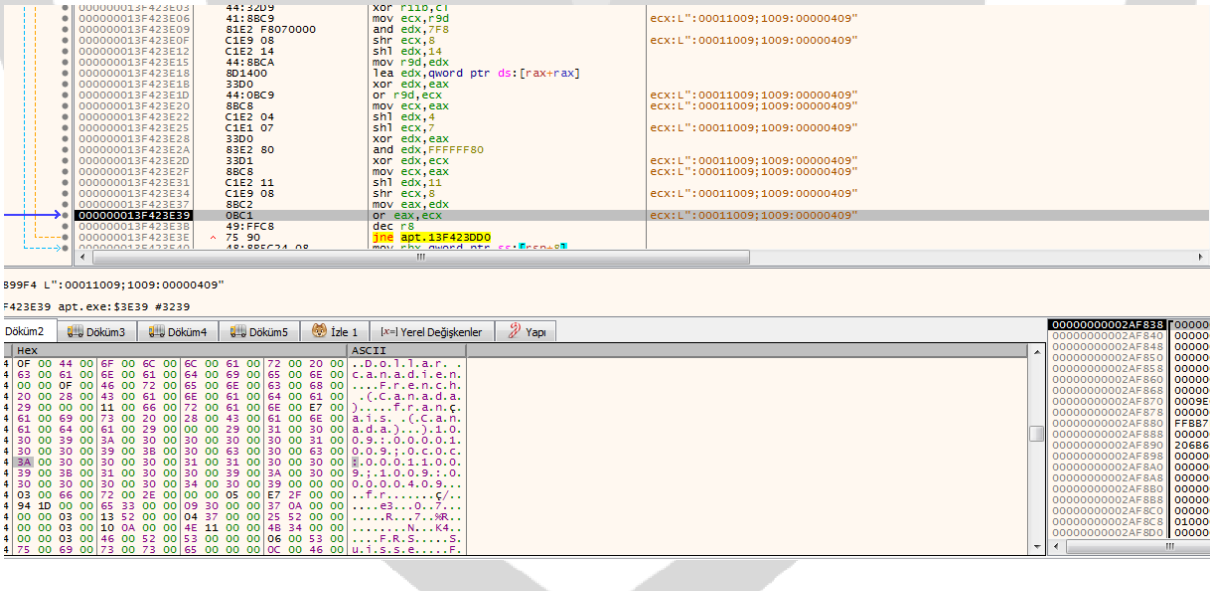


Sistem Bilgisi Alma

Zararlı yazılım kullandığı bilgisayarın wi-fi bağdaştırıcısının model numarasını almakta ve kendi sistemi içerisine yazmaktadır.

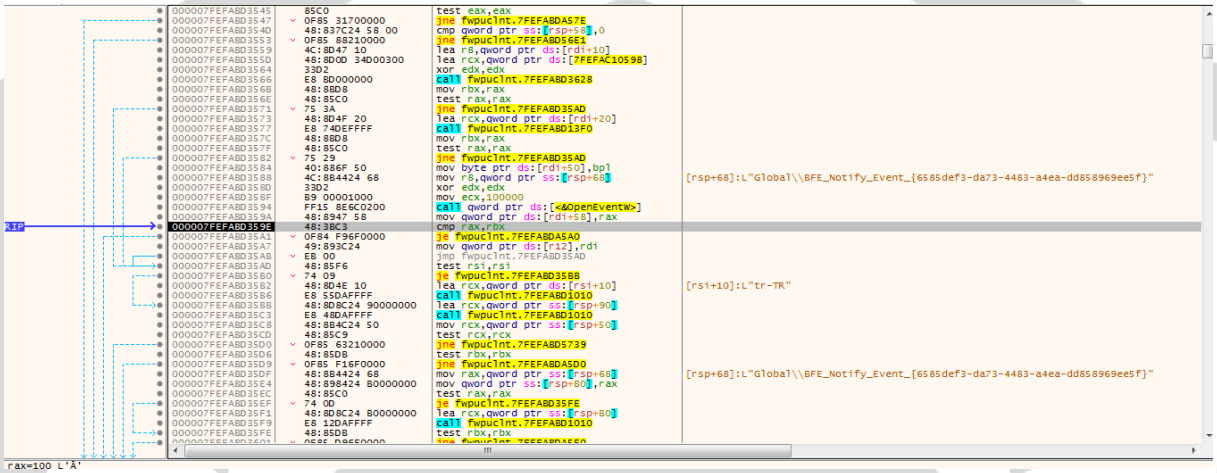


Giriş profilleri, girilen giriş dilinin ve girildiği klavyenin dilini ve bölgesinin otomatik olarak tanımlamasına yardımcı olmaktadır.

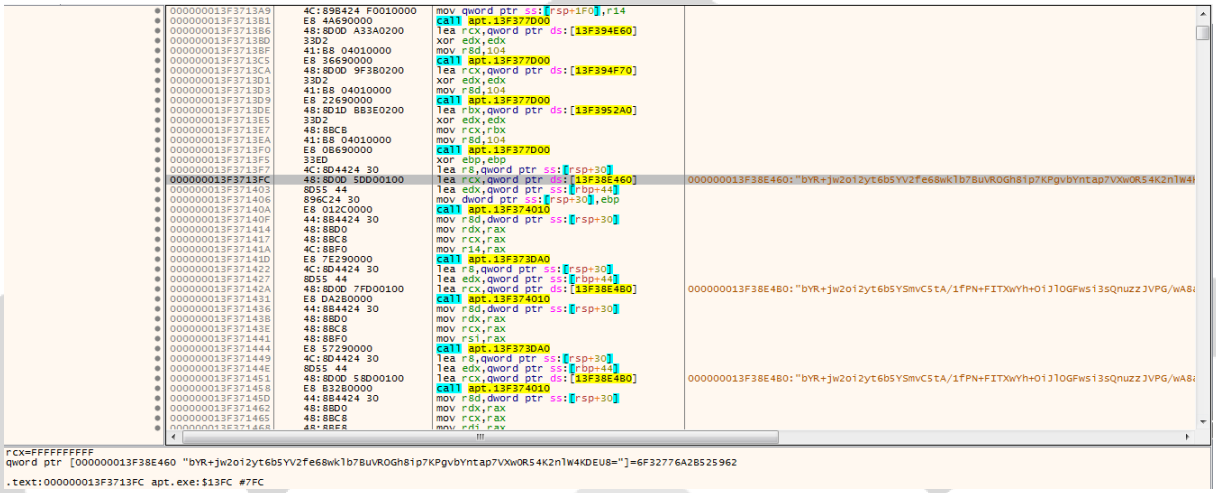


Event Altında Thread Başlatma

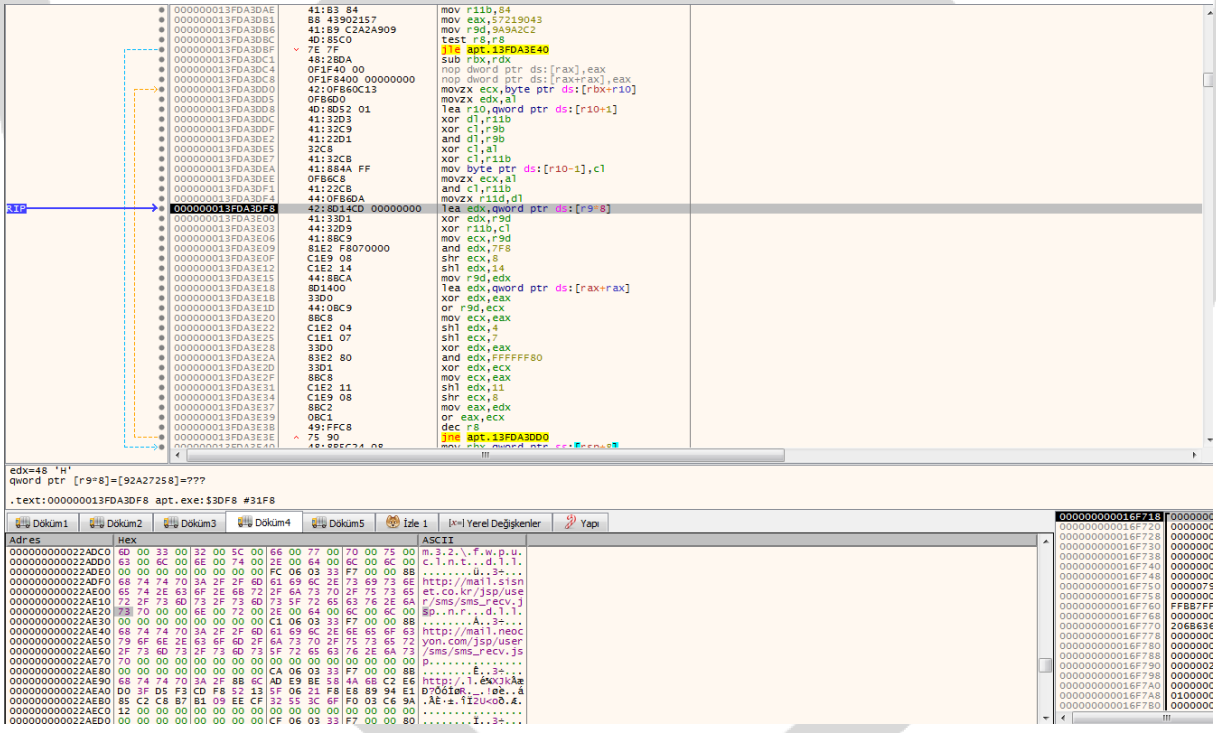
Zararlı yazılım “Global\\BFE_Notify_Event_{6585def3-da73-4483-a4ea-dd858969ee5f}” olay yürütme konfigürasyonu altında kontrol edip çalıştıracak olduğu thread’i bu komut satırı altından çalıştırmaktadır. Bu sayede analizini yapmayı zorlaştırmaktadır.



Bağlantı Kurduğu Adresler

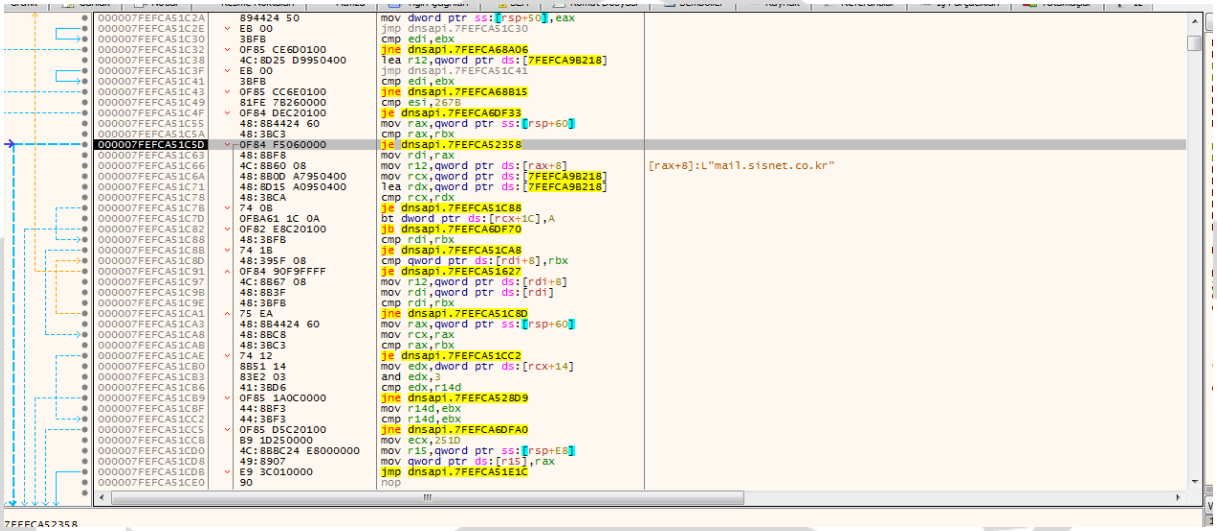


Encrypted halde tuttuğu URL bilgisini dinamik olarak çözümlemektedir. Çözümlenmiş URL bilgisi; “mail[.]sisnet[.]co[.]kr/jsp/user/sms/sms_recv_jsp” çözümlediği adrese bağlantı kurmaktadır. Bağlantı kurduktan sonra ise sistem üzerinde port açıp dinlemektedir.



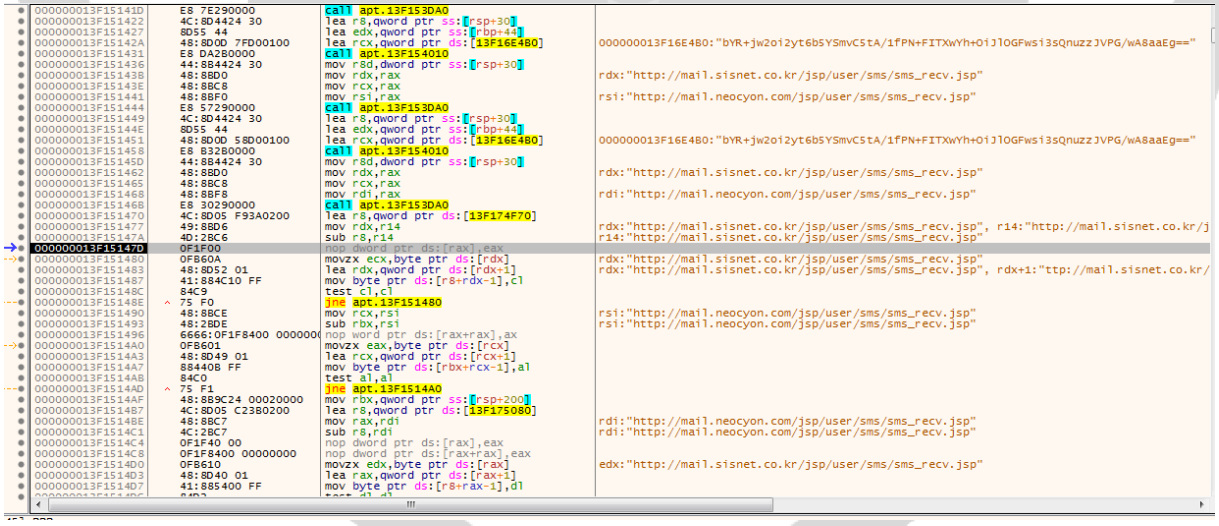
Bağlantı Kurduğu Adresler

Encrpyted adrese (“mail[.]sisnet[.]co[.]kr”) bağlantı kurmakta ve bir süre sonra bağlantıyı sonlandırmaktadır.



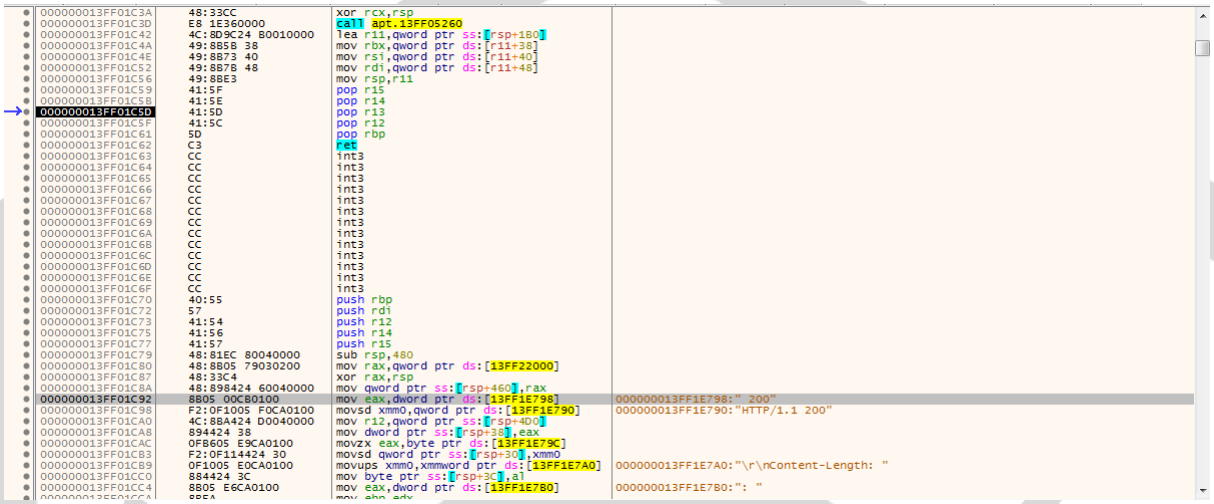
Bu adrese bağlantı kurmakta sonra ise tekrardan kullandığı sitenin url kısmını encrypt edip hafızasına yazmaktadır.

Tekrardan başka bir “mail[.]neocyon[.]com/jsp/user/sms/sms_recv.jsp” uzantısına bağlantı kurup dinlemekte ve kendi URL adresini encrpyt edip hafızasına yazmaktadır.



Bağlantı Kurduğu Adresler

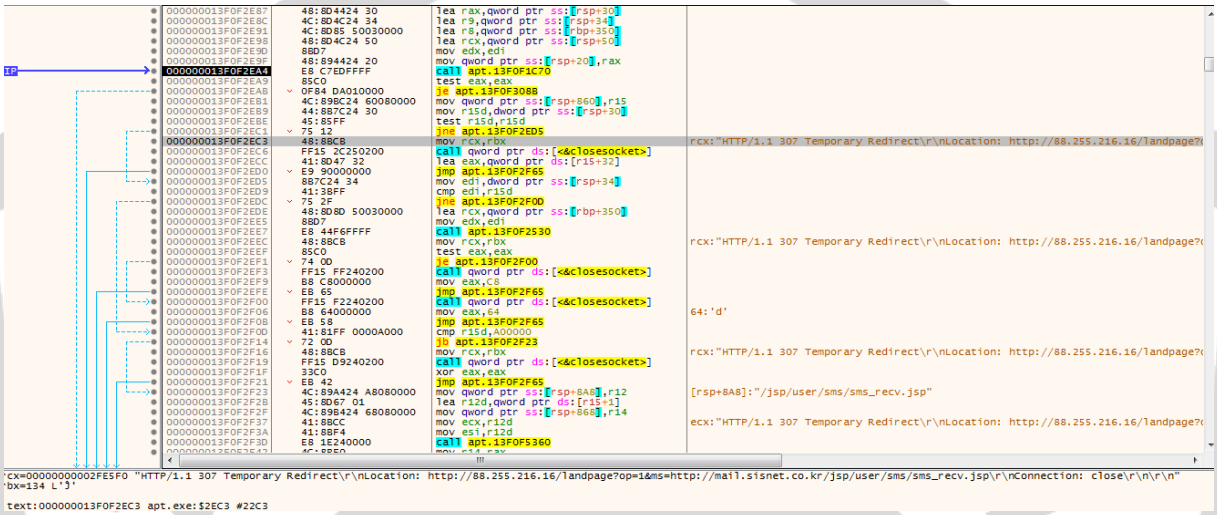
Zararlı yazılım “mail[.]sisnet[.]co[.]kr” adresine bağlantı kurduktan sonra server ile bağlantı kurduğunu onaylamak için sistem üzerinden HTTP/1.1 200 kodu gönderip bağlantıyı kurduğuna dair onay kodu göndermektedir.



Bağlantı kurduktan sonra ise her bağlantıya eşsiz birer cookie session id ataması yapmaktadır.

Bağlantı Kurduğu Adresler

Zararlı yazılım bağlantı kurduktan sonra 307 hatası verdirip yani internet sağlayıcısının taramasından kaçıp kendi sitesine yönlendirme yaptırtmaktadır. Böylece daha kolay şekilde kendi yaptıkları mail sitesine hata vermeden gitmektedir.

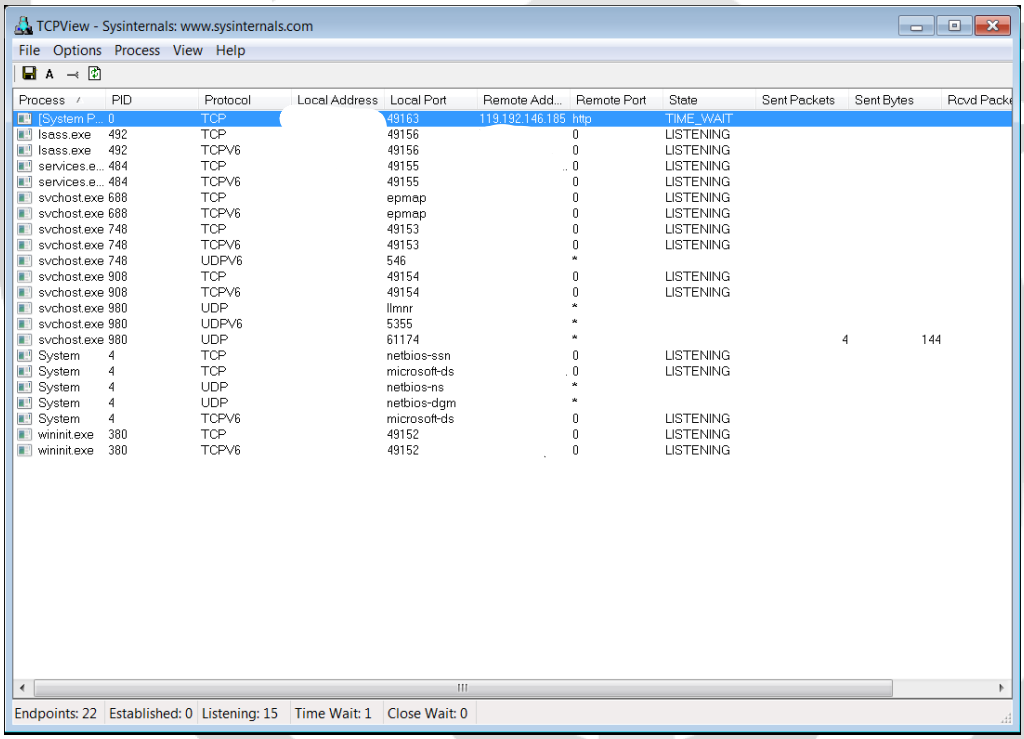


Network Analizi

İnternet sitelerine bağlantı kurduktan sonra ise 119[.]192[.]146[.]185 numaralı ip adresinin 80. portuna uzaktan erişimle bağlantı sağlamaktadır.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Por
[System Proc...	0	TCP		49201	119.192.146.185	http
[System Proc...	0	TCP		49202	119.192.146.185	http
[System Proc...	0	TCP		49203	119.192.146.185	http
[System Proc...	0	TCP		49204	119.192.146.185	http
[System Proc...	0	TCP		49205	119.192.146.185	http

Backdoor türünde bir zararlı yazılım olduğundan dolayı belirlenen ip adresinden komut beklediği için sürekli olarak bağlantı kurup bağlantıyı sonlandırmaktadır.



Mitre Att&ck Tablosu

Yürütme	Kalıcılık	Ayrıcalık Yükseltme	Savunmadan Kaçma	Keşif	Toplamak	Komuta ve Kontrol
T1059 Command and Scripting Interpreter	T1546.011 Application Shimming	T1055 Process Injection	T1497 Virtualization Sandbox Evasion	T1124 System Time Discovery	T1560 Archive Collected Data	T1573 Encrypted Channel
		T1546.011 Application Shimming	T1055 Process Injection	T1518.001 Securtiy Software Discovery	T1005 Data From Local System	T1105 Ingress Tool Transfer
			T1140 Deobfuscate Decode Files or Information	T1018 Remote System Discovery		T1071 Application Layer Protocol
			T1027 Obfuscated Files or Information	T1016 System Network Configuration Discovery		

Yara Kuralı

```
import "hash"
rule APT NukeSped: RAT
{
meta:
description = "n5JNGFT14Q.exe"
strings:
$str1= "mail.sisnet.co.kr/jsp/user/sms/sms_recv_jsp"

$str2= "mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
$str3=”bYR+jw2oi2yt6b5YSmvC5tA/1fPN+FITXwYh+OiJlOGFwsi3sQnuzzJVPG/wA8aaEg==”
$str4= "Global\\BFE_Notify_Event_{6585def3-da73-4483-a4ea-dd858969ee5f}"

$str5="bYR+jw2oi2yt6b5YV2fe68wklb7BuVROGh8ip7KPgvbYntap7VXw0R54K2nlW4KDEU8="

$str5= "119.192.146.185"

$command1 = "CreateMutexA"

$command2 = "Microsoft32"

$command3 ="GetProcAddress"

$command4 ="LoadLibraryA"
$command5 = "GetModuleHandleW"
$command6 = "DelayExecution"
condition:
hash.md5(0,filesize) == "fdc66cdabd46bc3b26aba4e59943726b" or all of them
}
```

Çözüm Önerileri

Backdoor türündeki Apt NukeSped zararlısından korunmanın yolları bulunmaktadır:

- Sistemlerde güncel, güvenilir bir anti-virüs yazılımının kullanılması,

- Gelen maillere özenle dikkat edilmesi, eklerin analiz edilmeden bilinçsizce

açılmaması,

- Spam maillerin dikkate alınmaması,

- Açılacak olan uygulamaların yönetici iznini manuel olarak yetkilendirme yaparken dikkat edilmesi,

- Mutex nesnelerinin sistem üzerinde oluşturulması gibi çözümler,

Backdoor türündeki Apt NukeSped zararlısının sisteme bulaşmasını engelleyebilmektedir.

BUĞRA KÖSE

https://www.linkedin.com/in/bugrakose/