# PurpleFox Exploit Kit

## Teknik Analiz Özeti

Analizlerimiz sonucunda bulunan PurpleFox Exploit Kit, zararlı yazılımı yöneten saldırganlar tarafından hedefe sızmak için kullanılır Metasploit benzeri bir yapısı vardır, içinde birden fazla Exploiti ve zararlı yazılımı yaymak için sofistike metotlar içerir. PurpleFox zararlısını diğerlerinden ayıran en önemli özellik Internet Explorer üzerinden hedef cihaz içinde kod yürütmeye olanak sağlayan 0day kullanması olmuştur (use-after-free CVE-2021-26411). Saldırganlar bu güvenlik açığını kullanarak hedef cihaza Phishing yöntemi ile bir URL gönderir, URL’e tıklayan kullanıcı saldırganlar tarafından hazırlanan ve zararlı yazılım içeren web adresine yönlendirilir, URL default web browser olarak otomatik olarak Internet Explorer ile açılır ise ve 0day tetiklenir ,bu aşmadan sonra hedef cihazda mshta ve powershell üzerinden zararlı yazılım aşamalar halinde çalışır.

## Purple Fox Yayılmasına Ait İstatistik Veri

Araştırmalarımız sonucunda bu yeni yöntemin çok hızlı bir yayılma hızına sahip olduğu gözlemlenmiştir. PurpleFox zararlısının yayılmak için tercih ettiği bir diğer yöntemin ise internet üzerinde Port taraması yaparak açık olan Windows SMB servislerini bularak SMB üzerinden kendini yaydığı gözlemlenmiştir. Guardicore Global Sensors Network’e dayanan bu veriler Purple Fox zararlısının yayılma hızının Kasım 2020 ve Ocak 2021 arasında %600 oranında arttığı ve toplam saldırı sayısının 90,000 ve üzeri olduğu biliniyor.

Graphical user interface

Description automatically generated with medium confidence

## Teknik analiz

## Kullanılan Exploit ve Shellcode

**Internet Explorer mshtml use-after-free (CVE-2021-26411)** güvenlik açığını kullanan saldırganlar araştırma sonucumuza göre Internet Explorer üzerinden hedef cihaz içinde açılan link ile uzaktan kod yürütme gerçekleştirir, bu güvenlik açığı Microsoft tarafından 9 Mart 2021 tarihinde keşfedilmiş ve yama edilmiştir. Sistemi Exploit etmek için gönderilen URL : **“ehektoe[.]lncnawgcidtia[.]xyz”**

Graphical user interface, text

Description automatically generated

JavaScript kodu içinde shellcode isimli bir değişken bulunur, Uint8Array ile encode edilmiş zararlı kodu içerir ve exploit çalışır ise hedef sistem üzerinde aktif olarak çalışır.

Text

Description automatically generated

JavaScript kodu içinde bulunan shellcode değişkeni, AES CBC ile şifrelenmiş ve Base64 ile encode edilmiş bir powershell scriptini içerdiği tespit edilmiştir.

A picture containing text

Description automatically generated

## Exploit POC

Resimde görüldüğü gibi hedef sistemde çalışan exploit ile Internet Explorer yazılımında use-after-free güvenlik açığını tetikler bu aşamadan sonra saldırganın belirlediği shellcode kod yürütülür eğer exploit içine zararlı bir kod konulmaz ise Internet Explorer hedef cihaz içinde çöker ve çalışmayı durdurur.

Graphical user interface, text, application, Word

Description automatically generated

POC İçin Örnek Exploit Kodu

Text

Description automatically generated with medium confidence

Exploit Çalışma Prensibi

1. Kaynak kod içinde HTML Element nesnesi (elem) ve Attribute nesneleri (attr1 , attr2) oluşur.
2. İki Attribute nesnesine nodeValue değer atanır, burada attr1’in nodeValue değeri, valueOf işlevinin aşırı yüklenmiş olduğu bir Object öğesine atanır (Pointer).
3. Attr1 ve attr2 adlı iki Attribute nesneleri elem nesnesine atanır .
4. Elem.removeAttributeNode (attr1) öğesini elem'den attr1'i kaldırmak için çağrılır.
5. RemoveAttributeNode methodu, valueOf işlevine bir geri çağrıyı tetikler, bu sırada, elem nesnesinin tüm nesnelerini (attr1 ve attr2) temizlemek için clearAttributes () çağrılır.
6. ValueOf return olarak döndüğünde, Internet Explorer memory üzerinde boş bir Pointer yüzünden çöker veya saldırgan tarafından oluşturulan shellcode boş olan Pointer’a Point edilerek sistem içinde RCE sağlanır.

Graphical user interface, application

Description automatically generated

Yukarıdaki PoC akış analizine dayanarak, çökme nedeninin valueOf geri çağırması sırasında clearAttributes() fonksiyonunun neden olduğu Double Free güvenlik açığı sonucuna varılabilir. Element nesnesi temizledikten sonra, yorumlayıcıya geri döner (yorumlayıcı düzeyinde silme işlemini iptal eder) ve tekrar serbest bırakır ve bu da Double Free ile sonuçlanır.

## Güvenlik Açığından Etkilenen Sürümler

Text

Description automatically generated with medium confidence

## Exploit Sonrası Zararlı Analizi

Zararlı yazılımı hedef sistem içinde çalıştırmak için exploit kullanan saldırganlar Anti Virüs ürünlerini bypass etmek için Powershell kullanarak dropper yöntemi ile zararlı yazılımı indirir ve çalıştırır, uzak sunucudan inen zararlı yazılım parçası Stenography yöntemi ile PNG formatlı bir dosya içinde saklanır, dosya formatı PNG olsa bile içeriğindeki String veriler zararlı yazılımın bir parçasını içerir.

**Adım – 1 :** Exploit tetiklenir ve zararlı yazılımı drop etmek için mshta yardımı sayesinde Base64 ile encode edilmiş Powershell scripti hedef cihaz üzerinde çalışır.

Graphical user interface, website

Description automatically generated

**Adım -2 :** Uzak sunucudan zararlı kod parçası içeren PNG formatında dosya “rawcdn[.]githack[.]net” adresinden hedefe cihaza indirilir , Stenography ile saklanan Powershell zararlı kod parçası PNG dosyası içinden Invoke-PSImage tekniği ile hedef sistemde çalışır.

Graphical user interface, website

Description automatically generated

Dropper Şeması

Zararlı yazılım çalıştığı işletim sistemine ve kullanıcı yetkisine göre farklı bir dropper ile sistem içinde çalışır. “rawcdn[.]githack[.]net” uzak sunucu adresinden “up.php?key={SAYI}” parametresi ile duruma uygun farklı zararlı yazılım parçaları indirilir, Reflective PE loader tekniği ile hedef sistem içinde çalışır ve yetki yükseltme exploitleri kullanarak (CVE-2020-1054 ve CVE-2019-0808 Privilege Escalation) Windows işletim sistemi içinde Admin yetkisi kazanır.

Diagram

Description automatically generated

Uzak sunucudan indirilen zararlı yazılım parçaları arasında (.ps1, .PNG ve .msi) formatları bulunur.

Table

Description automatically generated

Stenography ile Powershell zararlı kodunu gizleyen PNG formatındaki zararlı yazılım parçası örneği.

Graphical user interface, application

Description automatically generated

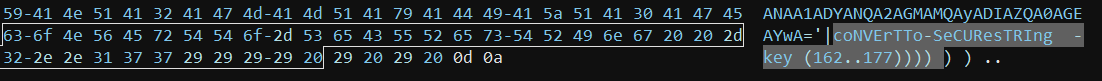
Powershell formatındaki zararlı yazılım parçası örneği.

A screenshot of a computer

Description automatically generated with low confidence

PurpleFox Powershell zararlısı encode edilme açısından Emotet ile benzerlik gösteriyor, Invoke-Expression için **“$vERBOsepreFErEncE.tOStRIng()”** ve String veriyi şifrelemek için **“ConvertTo-SecureString()”** gibi yöntemleri kullandığı tespit edilmiştir , analizlerimiz sonucu çok sıkı bir şekilde Obfuscate edilen Powershell scriptini açmayı başardık.

Obfuscate edilen veri ayrıca ikinci bir güvenlik katmanı daha sağlamak için AES ile Powershell zararlısına ait String verileri şifreliyor fakat şifreyi açmak için kullandığı yöntem şifreyi bize gösteriyor 162’den 177’ye kadar olan sayılar AES ile şifrelenen verinin şifresini gösteriyor.



Decode edilen veri analizlerimize göre PNG formatında başka bir zararlı parçasını indirmek ve işletim sistemi hakkında veri toplamak ile görevli. Stenography ile PNG içine gizlenen Powershell kodu execute ediliyor ve zararlının son aşaması olan Windows Installer (.msi) formatında sistem içinde çalışıp saldırgana ait C2’ye bağlantı sağlanıyor böylece döngü tamamlanıyor.

Graphical user interface, text

Description automatically generated

Analizlerimiz sonucunda edindiğimiz verilere göre zararlı yazılımın yapısı gereği işletim sisteminin özelliklerine göre farklı bir saldırı tekniği belirliyor ve uzak sunucundan buna uygun olan payload seçiliyor, bu durum MITRE ATT&CK teknik ve taktiklerine yansımış durumdadır.

Windows 7 MITRE ATT&CK

Graphical user interface

Description automatically generated

Windows 10 MITRE ATT&CK

Graphical user interface

Description automatically generated

## Process Tree

A screenshot of a computer

Description automatically generated

Windos 10 Cihazda PurpleFox Ağ Analizi

Text

Description automatically generated

Analiz sonucuna göre PurpleFox zararlı yazılımı matruşka bebek mantığı ile çalışır birden fazla katman ile kendini Anti Virüs ve EDR çözümlerine karşı korur bunu başarmak için birden fazla Obfuscation , şifreleme ve compres teknikleri ile son aşamaya gelene kadar asıl zararlı yazılımı gizler. Son aşamaya gelindiği zaman sahte bir Windows Installer ile uzak sunucudan zararlı yazılım verilerini indirmeye devam eder “M0021.cab” PurpleFox ShellCode içerir ve “6730A78E.moe” Nugget Phantom zararlısına ait ikinci farklı fazda bir zararlıya aittir.

Up.php?key=5 (Powershell)

Zararlının ilk aşaması, hedef sistemi tanımak ve sonraki aşamaya geçmek için PNG dosya uzantılı zararlı yazılımı uzak sunucudan indiren Powershell scripti.

Graphical user interface, text, application, Word

Description automatically generated

Up.php?key=7 (PNG)

Uzak sunucudan indirilen ve Stenography tekniği ile gizlenmiş Powershell komutları içeren PNG dosyası.

Text

Description automatically generated

Up.php?key=6 (MSI)

Son aşama olarak .msi dosya uzantılı zararlı yazılım hedef sisteme indirilir ve arka planda çalışır.

Application

Description automatically generated with medium confidence

Zararlı yazılımı geliştiren kişiye ait olabilecek pdb, dosya yolu geliştiren kişi hakkında bilgi edinmemize olanak sağlar.

Table

Description automatically generated

Uzak sunucudan indirilen zararlı .msi dosyası AV/EDR bypass için imzasız sahte sertifika kullanır.

Graphical user interface, text, application

Description automatically generated

Lateral Movement için SMB ve türevi servisleri kullanarak hedef ağ içinde açık Port taraması yapar.

Text

Description automatically generated

Aynı ağ içinden veya internet üzerinde açık ağlarda başka sistemlere yayılmak için PurpleFox SMB Port taraması yaptığı tespit edilmiştir.

Table

Description automatically generated

## PNG Stenography Analizi

Decode edilen PNG dosyası içinde Base64 ve Compress ile encode edilmiş şekilde Powershell kodu içerdiği tespit edilmiştir, zararlı yazılımın hedefi Anti Virüs ve EDR çözümlerine yakalanmadan en son zararlı kod parçasını (Up.php?key=6.msi) sistem içinde indirmek ve çalıştırmak, bu hedefe ulaşmak için sistem içinde 7-ZIP araması yapıyor 7-ZIP yazılımı içinde yer alan Compress özelliğini kullanarak AV/EDR çözümlerinden gizlenmek için ikinci bir katman daha oluşturuyor.

Graphical user interface, text, application, email

Description automatically generated

PNG içinde gizlenen en önemli bulgulardan biri bu sofistike zararlı yazılımın hedef sistem içinde ms15-051 (CVE-2015-1701) olarak bilinen bir Admin yetki yükselteme exploiti kullanması olmuştur, bunu başarmak için Powershell ile Base64 encode edilen exe dosyasını hedef sistem içinde yine Powershell ile çalıştırdığı tespit edilmiştir.

Text, letter

Description automatically generated

Analiz için Base64 decode edildiğinde zararlı Powershell kodunun ms15-051 güvenlik açığını hedef sistem içinde zafiyeti taramak ve exploit işlemi gerçekleştirmek için kullandığı fakat test için kullandığımız sistemin Windows 10 işletim sistemine sahip olduğundan ms15-051 den farklı olan (CVE-2021-1732) yetki yükselteme zafiyetini kullandığı tespit edilmiştir.

Microsoft Windows - Local Privilege Escalation (CVE-2021-1732)

A picture containing text, keyboard

Description automatically generated

Microsoft Windows - Local Privilege Escalation MS15-051 (CVE-2015-1701)

A picture containing text, computer, keyboard

Description automatically generated

## IOC Verileri

**Hash (MD5)**

6467874D952A5FFC1EDFD7F05B1CC86D

36061CB651C281053960FB15610CCBD4

43BA54DA3940E5B35386F521FAEDBC2D

7378ADD5A75507A691B3E784056A4438

3C519C775638B77CA833EDF550DDE4A3

682F980368BD7151325F822F516DD8CD

D879A16A9FC062F9DAC93D523FD625D4

91F2CB9F92C6BEB7CD262E98918879F4

300E77DBA5AA6F943779C58338F8E0D9

073D6D148034712997A0A12EDD988344

FF3DA3D998BF86B8C51F9F84ED6A21F3

7E1B8AC1DF811A5561871FC9F05AF7EE

32FB30A5F5871C3C5C50DBD5812BC610

**Ağ Trafiği**

ehektoe.lncnawgcidtia.xyz

lingering-math-ec29.7axrg.workers.dev

rawcdn.githack.net

103.44.239.201:19125

222.73.247.91:18812