UKRAYNA-RUSYA SAVAŞI BAĞLAMINDA SİBER GÜVENLİK EKOSİSTEMİ'NDE YAŞANAN GELİŞMELER VE DEĞERLENDİRMELER

Bahtiyar Münir PALTACI

ÖZET

Günümüzde yaşanan teknolojik gelişmelerin siber ekosistemdeki payı incelenerek Rusya ve Ukrayna arasında yaşanan kriz ve ardından krizin sıcak savaşa dönmesi sonucunda ortaya çıkan siber savaşın bu ekosistemdeki payı göz önünde bulundurularak kapsamlı bir değerlendirme hedeflenmektedir.

Bu kapsamlı çalışmanın amacı, Ukrayna-Rusya savaşı sırasında ve öncesinde iki ülke arasında siber alanda yaşanan saldırılar ve hacker gruplarının bu saldırıları nasıl kullandığı, kimlerden destek aldığı, ne tür etkiler oluşturduğu, savaşın içerisinde ne tür yönlendirmelerde veya kalıcı etkilerde bulunduğu gibi sorulara cevap aramaktır, aynı zamanda gündeme yansıyan saldırı türleri, hacker grupları ve bunları kullanan devletler gibi konularda da detaylı açıklamalara ulaşıp sonuç çıkarmaktır.

Gelişmeler boyunca iki tarafında yapmış olduğu siber saldırılar incelenmiştir. Ekosistem içerisinde bulunan mevcut zafiyetlerden yanı sıra yeni bir siber saldırı türü olup olmadığı gibi konular araştırılarak kıyaslamalar yapılmıştır. Aynı zamanda kritik altyapılar, devlet kurumları, özel sektör gibi alanlar incelenerek her iki tarafında bu alanlarda siber olarak kayıplar yaşayıp yaşamadığı ve detayları irdelenmiştir.

Tüm bu araştırmaların sonucunda varılacak sonuç, Rusya-Ukrayna siber savaşının dünya genelinde etkileri ve yaşanan siber gelişmeleri toparlayarak gün ışığına çıkarıp bir bütün halinde inceleme fırsatı oluşturabilmektir.

Anahtar Kelimeler: Siber Güvenlik, Siber Savaş, Rusya-Ukrayna Savaşı

GİRİŞ

William Ford Gibson'un da romanında (Neuromancer) kullandığı bir deyim olan Cyberspace (Siber Uzay) olgusu tarihte ve günümüzde çeşitli siber kavramlar meydana getirmiştir. Dünyanın değişen politikalar veya modernleşen unsurlar içerisinde kendi gelişimlerini ve yenileşim süreçlerini kapsayan değerlerin; sağlık, ekonomik, ticari, askeri, eğitim gibi ana konular olduğunu rahatlıkla söyleyebiliriz. Kimi ülkelerde bu kavramlar belli bir kalıba oturmuş olup kimi ülkelerde ise değişimsel olarak verilere dayanmaktadır. Bunlar da gelişmiş ve gelişmekte olan ülkeler olarak tanımlanmaktadır.

Günümüzde IT alanında yapılan çalışmalar; yazılımlar, donanımlar ve bunların oluşturduğu projeler ve uygulamalar teknolojik olarak sürekli kendini yenilemektedir. Robotik alandan, askeri alana, askeri alandan devlet içi kurumsal iletişime kadar uzanan; bir diğer ifadeyle bilginin işlenmesi ve kaydedilmesi/tanımlanması vasıtasıyla oluşan her bir ağ trafiğinin oluşturduğu ortam siber ortam/siber uzay olarak ifade edilir. Evrende nasıl Dünya,Mars,Jupiter gibi gezegenler varsa siber uzay da da çeşitli tanımlamalar vardır. Basit bir ifadeyle ve karşılaştırmayla düşünecek olursanız evren = siber uzay , gezegenler = bilişim teknolojileri, bilgi teknolojileri, ham/işlenmiş bilgi ve/veya ağ trafikleri olarak yorumlanabilir.

Bazı kaynaklarda Pentagon'un yıllar içerisinde Siber Uzayın ne olduğuna dair en az 12 adet tanım açıkladığından bahsedilmektedir. 2008 yılındaki son tanımında : "İnterneti de içeren bilgi bilgi teknolojileri alt yapılarının bağımsız ağı, telekomünasyon ağı, bilgisayar sistemleri ile gömülü işlemciler ve yöneticileri içeren bilgi ortamı dahilindeki küresel alan" olarak tanımlandı (Singer ve Freidman, 2015).

Ülkemizde Ulusal Siber Güvenlik Stratejisi belgesinde yayınlanan Siber Uzay kavramı : "Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam" şeklinde ifade edilmektedir (Ulaştırma, Denizcilik ve Haberleşme Bak. 2019).

Teknolojik olarak bu olaya yaklaştığımızda, siber uzay kavramı ilk paragrafta bahsettiğimiz yenileşim ve gelişimlere dayanarak ve yeni bir akım oluşturarak dünya genelinde siber güç tanımını oluşturmuştur. Bu siber güç tanımı ise hiç şüphesiz, Eğitim,

Sağlık, Askeri, Ticari, Ekonomik v.b unsurların tamamı ile ilişkilidir. Bir ülkenin kalkınması için gerekli olabilecek tüm unsurların içerisinde mutlak bir siber güç kavramı geçmektedir.

Siber Uzay içerisinde yer alan Siber Savaş kavramında ülkeler arası yapılan siber saldırılar ve savunmalar söz konusudur ve ülkelerin gelişmişlik seviyelerine göre de siber güç potansiyelleri ortaya çıkar. Bu hususta 24 Şubat 2022 tarihinde resmi olarak başlayan Rusya – Ukrayna savaşı bağlamında iki ülkenin de siber güç potansiyellerini göstermeleri açısından ortaya bir fırsat çıkmıştır. Her iki ülkenin de devlet destekleri hackerları ve siber ordusu tarafından birbirlerine yapmış olduğu siber saldırılar olmuş hatta kontrolden çıkan bazı hacker grupları dünya genelinde Avrupa ülkelerine de siber saldırılar yapmıştır.

İnternetin karanlık yüzü olarak bilinen Dark Web içeriklerinde, TOR ve benzeri yazılımlar ile ulaşım sağlanan çeşitli hacker forumları veya ortamlarında Rusya tarafından gerçekleştirilen siber saldırılarda zirveye çıkan hacker grupları olmuştur. DDOS saldırıları, zararlı yazılım ile fidye saldırıları, SQL ve türevi saldırılar user-pass bilgilerine erişip sayfa indexleme, sosyal mühendislik, phishing çeşitlerine kadar siber alanda kullanılan yöntemlerin çoğu bu siber savaşta da gerçekleşmiştir.

Dolayısıyla, gerçekleşen bu siber saldırıların iki ülke nezdinde kritik altyapılara, devlet kurumlarına, gizli bilgilere, ulusal güvenliğe, toplumsal düzene verdiği zararlar bakımından inceleme fırsatı doğmuştur. Aynı zamanda Rusya-Ukrayna savaşının getirdiği siber savaşta dünya genelinde siber güvenlik ekosisteminde yaşanan gelişmelere doğrudan etkisi olmuştur.

Siber Savaş, Kategorilendirme, Sınıflandırma, Hukuksal Boyut

Gerçek bir savaş durumu ile "savaş" konseptinin çok daha sık olan kullanım ve yanlış kullanımları arasındaki kopukluğun "siber savaş" gibi bir terimi tartışırken akılda tutulması çok önemlidir. Savaş, uluslararasındaki silahlı çatışmalardan (İkinci Dünya Savaşı) sembolik çekişmelere (New York şehrinin "şekerle savaşı") kadar çok çeşitli durum ve davranışlar kümesini tanımlamak için kullanılmaktadır. "Siber savaşa" gelince, terim bir siber barbarlık ve bozulma kampanyasından (çoğunlukla "Rus-Estonya siber savaşı" olarak adlandırılan) gerçek bir siber araçlardan faydalanan savaş durumuna kadar her şeyi tanımlamak için kullanılmıştır (Singer ve Freidman, 2015).

Fakat siber savaşın ne zaman başladığını ve bittiğini bilmek, onu tanımlamaktan daha zor olabilir. Çoğu savaşın, gerçekte İkinci Dünya Savaşı'nın olduğu gibi açık başlangıç tarihi ve anlaşmalı bitiş tarihi yoktur. Bunun yerine, başlangıç ve bitişleri bulanıktır. Örneğin ABD 1950'de Kuzey Kore'ye savaş ilan etmemiş olabilir fakat 5.3 milyonun öldüğü bir çatışmanın Başkan Truman'ın zamanında adlandırdığı gibi sadece bir "polisiye eylem" olduğunu tartışmak zordur. Bunu takiben, tarih kitaplarının belirttiği gibi Kore Savaşı resmi

olarak bir barış anlaşmasıyla hiçbir zaman sona ermediği halde, gerçek çatışma 1953'te durmuştur. Siber savaşın çizgileri de o kadar bulanık olabilir. ABD Ulusal İstihbarat Başkanlığı'nın altındaki karşı istihbarat birimin başı olan Joe Branner şöyle söylemektedir: "Biz ABD'dekiler, savaş ve barışı bir açma kapama düğmesi olarak -ya topeykün savaşın ya da barışını tadını çıkartan- düşünme eğilimindeyiz. Gerçek farklıdır. Biz şu anda nadiren açık savaşta olan ulusların arasında sürekli bir çatışma halindeyiz. Kesinlikle savaş halinde olmadığımız Çin gibi ülkelerin bile bizimle yoğun bir siber çatışmanın içinde olduğunu anlamamız gerekir" (Singer ve Freidman, 2015).

Siber savaşlar stratejik, operatif ve taktik olmak üzere her seviyede uygulanabilir olma özelliğine sahiptir. Bu nedenle her seviyede istenen etki elde edilebilmektedir. Hedef olarak ise siber savaşlar, temel olarak ülkelerin kritik bilgi sistem altyapılarını hedef almaktadır. Siber savaş sayesinde bu altyapıların hizmet dışı bırakılmasının yanı sıra ülkelerin sivil ve askeri hassas ve kıymetli bilgilerine ulaşabilmekte, soz konusu bilgiler çalınabilmekte hatta silinebilmektedir. Ayrıca saldırıya maruz kalan ülke halkını ve yönetimini, siber ortamda dezenformasyon ile psikolojik olarak etkilemek de mümkün olmaktadır. Bu nedenle toplumun her kesimini etkileyebilmekte, çatışma ve rekabet ortamı yaratabilmektedir (Bayraktar, 2015).

Gerçekleştirilmek istenen amaçlar dikkate alındığında siber savaş; ekonomik, politik, askeri veya psikolojik amaçlar için hedef seçilen ülkeye yönelik bilgi ve iletişim sistemleri üzerinden gerçekleşen organize saldırılar bütünü olarak tanımlanmaktadır (Tatar ve Matarcıoğlu, 2010).

Siber Savaşlar amaçları dikkate alındığında üç ana başlık altında sınıflandırılmaktadır. Bunlar Tablo-1 de gösterilmiştir.

	Motivasyon	**Hedef Kitle**	**Metotlar**
Siber Savaş	Askeri, Siyasi ve Ekonomik Fayda	Kritik Bilgi Sistem Altyapıları, Askeri Bilgi Sistemleri, Devletler, Kurumlar, Firmalar	Siber Taarruz Yöntemlerinin Kullanımı
Siber Casusluk	Kritik Bilgi Kazanımı, Askeri ve Ekonomik Fayda	Askeri Bilgi Sistemleri, Devletler, Kurumlar, Firmalar	Güvenlik Açıklarının Kullanımı
Siber Terör	Siyasi Fayda	Devletler	Bilgisayar Tabanlı Şiddet ve Tatmin
Siber Sabotaj	Ekonomik Fayda, Kişisel Tatmin	Devletler, Kurumlar, Firmalar	İnsan Faktörünün Kullanımı

Tablo-1: Siber Savaşların Sınıflandırılması

Siber savaşlar klasik savaşlara göre kıyaslandığında farklı üstünlükler söz konusu olabilmektedir. Asimetrik bir savaş olarak değerlendirilen siber savaşlarda kullanılan silah sistemleri hayati riskler oluşturabilmektedir. Klasik savaşlarda kullanılan silah sistemlerinin

maliyetleri yüksek olmakta ve ileri teknolojiye ihtiyaç duyulmaktadır. Aynı zamanda kullanıcılarının ölüm riski de bulunmaktadır. Bunun yanında siber savaşlarda kullanılan silah sistemleri çoğunlukla bir bilgisayara sahip olma maliyeti gibi oldukça düşük maliyetli olmasına karşın, etkisi bir o kadar yüksek maliyetli ve zarar vericidir (Bayraktar, 2015).

Tablo-2 de klasik savaş ve siber savaş arasındaki farklar ve karşılaştırmaya yer verilmiştir

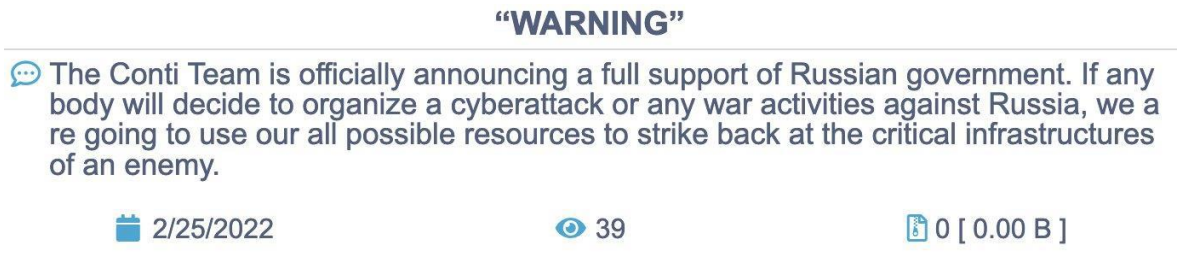
Kriterler	Klasik Savaş	Siber Savaş
Saldırı Kaynağı	Saldırıların nereden geldiğinin bulunması kolaydır.	Saldırıların nereden geldiğini tespit etmek çok zordur. Hatta bazen imkansızdır.
Hızı	Bir füzenin, bir uçağın, tankın veya muharebeye dahil olan başka bir silah sisteminin hızı kadardır.	Işık hızındadır.
Hasar Tespiti	Fiziksel etkilerinden dolayı hasar tespiti nispeten kolaydır.	Nerede ve ne kadar hasar oluştuğunu tespit etmek çok zordur. Çoğu zaman imkansızdır.
Silah Sistemleri	Tabanca, top, tüfek, bomba, uçak, gemi, tank, füze, radar v.b	Çipler, bilgisayarlar, veya bilgi sistemlerinde kullanılan diğer donanımlar, yazılımlar.
Teknoloji İhtiyacı	Genelde ileri teknoloji gerektirmektedir.	Zaten mevcut olan bilgisayarın da kullanılması mümkün olduğundan çoğunlukla çok yüksek teknik teknolojiye ihtiyaç duyulmamaktadır. Ancak, etkili olabilmek için yüksek teknolojinin kullanılması da faydalıdır.
Maliyeti	Kullanılan silah/sistemlerin maliyetine bağlıdır. Pahalıdır.	Genelde çok ucuzdur. Bazen bir bilgisayarla etkili olmak mümkündür.
Etkisi	Çoğunlukla fiziksel alanda etkilidir.	Çoğunlukla bilgi ve iletişim sistemleri alanında etkilidir.

Tablo-2: Klasik Savaş ve Siber Savaş Arasındaki Farklar

Diğer bir önemli nokta olan Siber Savaş'ın hukuksal boyutu literatürde uluslararası alanda gerçekleşen klasik savaş kurallarıyla aynı olarak gösterilmektedir. Fakat kuralların uygulanabilirliği tartışmaya açıktır.

Ortak savunma anlayışının siber alanda da geçerli olduğu fikri ve girişimi bir çok uluslararası belgede ifade edilmiştir. Estonya'nın başkenti Tallinn'deki CCDCOE'nin bir grup uzmana yazdırdığı ve 2013 yılında tamamlanan "Siber Savaşta Geçerli Uluslararası Hukuk üzerine Tallinn Makaleleri" adlı rapor bilim adamı ve uzmanların olması gerekeni değil cari uluslararası hukuku baz alarak konuya ilişkin yaptığı değerlendirmelerini yansıtmaktadır. Temel olarak siber ortamdaki savaş hukukunu analiz etmekte; "kuvvete başvurma hakkı" (egemenlik, devletin sorumluluğu, güç kullanımının yasaklanması ve meşru müdafaa, vb. konuları) ve "savaşta geçerli kurallar"ın (tarafsızlık hukuku, meşru hedefler, orantılılık,) siber alana nasıl uyarlanacağını incelemektedir. Uluslararası savaş hukukunda geçerli kurallar siber ortamda da aynen geçerlidir (Bilişim İnovasyon Derneği, 2022).

Siber Savaş'da yaşanan saldırılara bakıldığında hukuk kurallarının uygulanabilirliği konusunda bazı boşluklar bulunmaktadır. Zira hacker gruplarının doğrudan devletin desteğini aldığı kanıtlanmadığı sürece ülke nezdinde siber bir saldırı yapıldığı da kanıtlanmayacaktır. Bunun en büyük örneği RF devlet başkanı Vladimir Putin'in savaş öncesinde gerçekleşen siber saldırılarda devlet destekli olduğu bilinen hacker gruplarına "milliyetçi gençler" diyerek devletin desteğini almadığı konusunda vurgu yapmış olması ve devleti, yapılan siber saldırılarda sorumluluktan uzak tutmasıdır. Şekil-1 de devlet destekli olduğu bilinen Rus hacker "Conti" grubunun Rusya'ya yapılacak siber saldırılara misilleme yapacağını gösteren bağımsız* açıklaması verilmiştir.



Şekil-1: Conti hacker grubunun misilleme uyarısı

RF-UK Savaşı Başladığında Siber Ekosistem'de Yaşanan Gelişmeler

24 Şubat 2022'de UK-RF savaşı resmen başladı. Siber uzayın akışkanlığı savaşın başlangıcında başlamış ve bugüne kadar devam etmektedir. Bir siber savaş durumunda, ülkenin kritik altyapılarından biri veya birkaçı bozulabilir. Ukrayna-Rus savaşının ağ boyutu dikkate alındığında aşağıdaki istatistikler elde edilmiştir:

1. Rusya'da bir dağıtılmış hizmet reddi (DDOS) saldırısında yaklaşık 17.000 IP adresi tespit edildi.
2. Yaklaşık 70 hükümet web sitesi saldırıya uğradı.
3. Ukrayna'yı destekleyen ve ilgili Telegram kanallarına abone olan bilgisayar korsanlarının sayısı 265.000'i aştı.
4. Dünya çapında 60'tan fazla hacker grubu bu savaşta rol oynadı.
5. Savaş sırasında 50'den fazla CVE (Ortak Güvenlik Açıkları ve Etkilenmeler) kullanıldı (Tubitak Bilgem, 2022).

3. maddede belirtilen Ukrayna'yı destekleyen gönüllü hacker gruplarının sayısının 265.000'i aşmasında Ukrayna Başbakanı Mykhailo Fedorov'un açılan Telegram grubuna çağrı yapmasının etkisi büyüktür. Bu kapsamda devlet destekli bir hacker ordusu oluşturulmuş veya varolan devletin siber gücüne gönüllü birlikler alınmıştır denilebilir. Savaş durumunda devletin açıkca hacker grupları kurması da bu kapsamda RF-UK savaşında bir ilk olarak görülmektedir.

Mykhailo Fedorov'un açıklaması : "Bir BT (Bilişim Teknolojileri) ordusu yaratıyoruz. Dijital yeteneklere ihtiyacımız var. Tüm operasyonel görevler burada verilecektir. https://t.me/itarmyofurraine. Herkes için görevler olacak. Siber cephede savaşmaya devam ediyoruz. İlk görev, siber uzmanlar için kanalda." olarak resmi kanallarda yer almaktadır. Şekil-2'de Mykhailo Fedorov'un 26 Şubat 2022'de Twitter üzerinden yapmış olduğu bu açıklama gösterilmiştir.

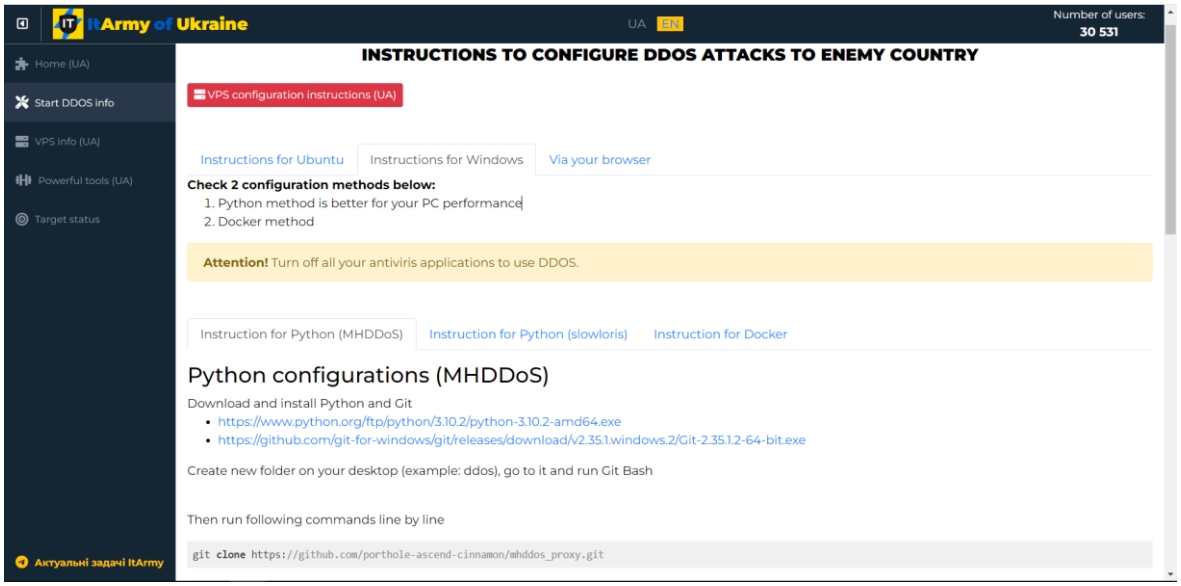
Şekil-2: Mykhailo Fedorov'un 26 Şubat 2022'de Twitter üzerinden yapmış olduğu açıklama

İlgili Telegram grubunun üye sayısı anlık olarak (17.04.2022, 01:05) 291.844 olarak görülmektedir. Ayrıca Telegram kanalında RF hükümetine ait birçok web adresi bulunmaktadır ve hedef olarak gösterilmektedir. Yine .ru uzantılı birçok web sitesi olmakla birlikte bu web sitelerinin IP adresleri açık TCP portları gibi bilgiler de yer almaktadır/hedef olarak gösterilmektedir. Bu web siteleri arasında çevrimiçi TV akış hizmetleri, Rus haber ajansları, aktif Rus şirketler gibi yapılar bulunduğu gözlemlenmiştir.

Ukrayna'nın siber cephede dünya genelinden herkese ulaşabilmesi ve devlet destekli olarak gruplar kurması Rusya'nın almış olduğu siber saldırıları çoğalttığı gibi Ukrayna'nın atmış olduğu bu adım siber ekosistemde önemli bir gelişme olarak görülmektedir. Daha önce açık biçimde dünya genelinde hackerlardan destek toplayan resmi bir devlet olmamıştır.

IT ARMY of Ukraine isimli Telegram kanalının aynı zamanda bir internet sitesi de olduğu görülmektedir (https://itarmy.com.ua). Bu web sitesinde Rusya kaynaklı hedeflerin imha durumları ve bu hedeflere yapılan saldırıların son kullanıcılar tarafından nasıl yapılacağına dair teknik-eğitim metaryelleri görülmektedir. Kaynak taraması yapıldığında dünya genelinde ilk olarak gizli saklı bir yönü kalmaksızın devlet destekli olup karşı devlete karşı yapılan siber saldırılarda eğitim-teknik destek verilen ve karşı devlet dijital sistemlerinin imha durumları, kayıtları, güncel adresleri gibi konularda bilgi sağlayan web siteleri arasında yine bir ilk olarak görülmektedir.

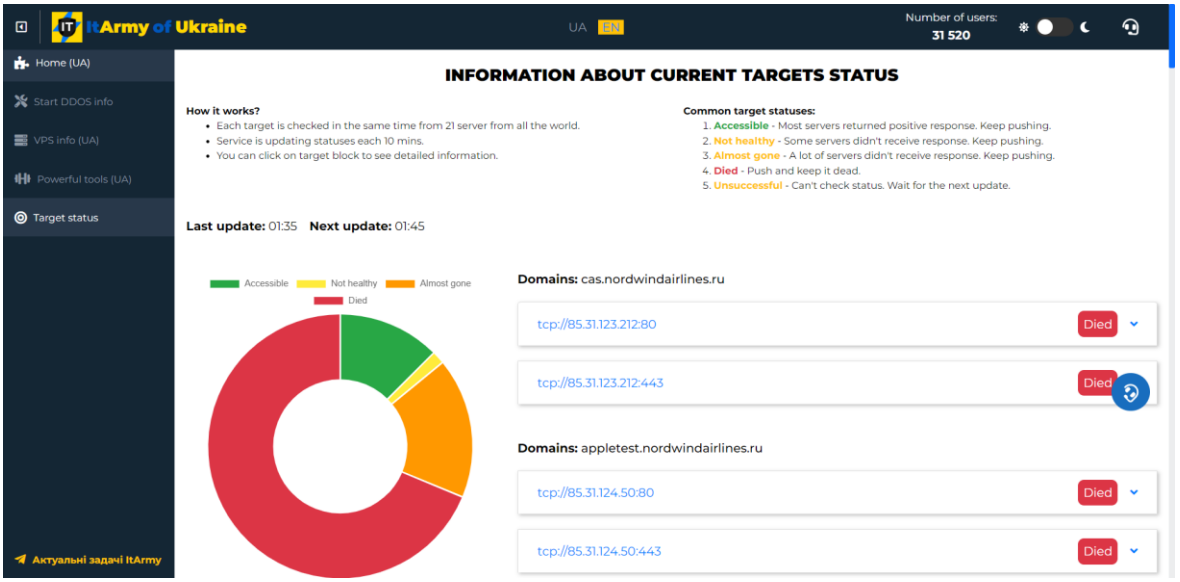
Şekil-3'de verilen görselde IT Army of Ukrania isimli web sitesinde yer alan "Düşman Ülkeye DDOS Saldırılarını Yapılandırma Talimatları" isimli başlıkta DDOS saldırılarının nasıl gerçekleştiğine dair Windows ve Ubuntu sistemlerde teknik bilgiler verildiği gösterilmiştir.



Şekil-3: Devlet destekli oluşumda (IT Army of UK) düşman devlete karşı nasıl siber saldırı yapılacağını gösteren talimatlar

Şekil-4'de verilen görselde IT Army of Ukrania isimli web sitesinde yer alan "Mevcut Hedeflerin Durumu Hakkında Bilgi" isimli başlıkta düşman ülkenin (RF) web

sistemlerinin IP adresleri ve domain bazında gerçekleşen saldırılar kapsamında aktif-pasif durumları gösterilmiştir. IP adresi ve domainler olarak listelenen sistemlerin aynı zamanda IT Army of Ukrania adlı Telegram grubunda paylaşılan hedefler olduğu tespit edilmiştir.



Şekil-3: Devlet destekli oluşumda (IT Army of UK) düşman devlete karşı gerçekleştirilen siber saldırıların durumları hakkında verilen bilgiler

Toplanan kaynaklara bakıldığında açık biçimde görülmektedir ki dünya genelinden resmi devletere savaş durumunda destekler gelmektedir. Dünya genelinin haklı gördüğü devlete karşı gerçekleştirdiği yardımlar arasında siber ekosistemde gerçekleşen yardımların etkisi büyük olmuştur. Gerekli kamuoyu oluşturularak mağduriyet durumları ve haksız yere işgal gibi faktörlerle savaşta destek alınabilmektedir. Siber ekosistemde bu yardımlar ile siber savaşın klasik savaşa göre daha kolay ve her yerden yapılabilmesi göz önünde bulundurulduğunda, bu kapsamda siber savaş faktörünün ne derece etkili olduğu unutulmamalıdır. Araştırmamızda bir kez daha dikkat çekmektedir ki bu hususlar; siber savaşın her türlü, her yerden, tespit edilmesi zor şekillerde istenilen hedefe yapılabiliyor olması ve bunun sonuçlarının başka olumlu ve hayati sonuçlara sebebiyet verebilme kapasitesi olmasıdır.

Çoğunlukla Ukrayna merkezli bu saldırıların siber dünyayı ikiye böldüğü görülmektedir. Conti olarak bilinen fidye yazılımı grubunun Ukraynalı üyesi 13 ay önce ekipte yaptığı konuşmayı kamuoyuyla paylaşırken, dünyaca ünlü hacker grubu Anonymous da Rusya Savunma Bakanlığı'na karşı olduğunu iddia ederek Rusya'ya siber savaş ilan etmiş ve saldırılardan sorumlu olduğunu iddia etmiştir. Buna ek olarak, Anonymous'un Rus hükümetine ait çok sayıda kanalın ve Ukrayna yanlısı yayınların ele geçirilmesinde parmağı olduğu bilinmektedir (CyberMag, 2022).

Anonymous hacker grubu genellikle DDOS olarak bildiğimiz hizmet dışı bırakma saldırıları ile Rusya'nın birçok kamu kurumuna ve uzantılarına siber saldırı gerçekleştirmiştir. Şekil-5'de verilen görselde Anonymous grubunun Ukrayna halkına övgüleri ve siber alanda yanında olduklarına dair bildirgeleri görülmektedir.

Şekil-5: Siber Alanda Ukrayna tarafında olduğunu ilan eden Anonymous hacker grubu

Açıkça taraf belirten hacker gruplarının taraf belirttikleri ülkelere karşı destek sağlamaları sebebiyle taraf belirtilen ülkenin düşmanı olan ülke veya ülkeler tarafından karşı saldırıya uğramaları da söz konusu olabilmektedir. Çoğunlukla savaş durumu olsa da olmasada herhangi bir toplumsal olaya karşı hacktivist saldırılarıyla bilinen Anonymous grubu daha önce yaşanan gelişmelerde ülkelerin iç işlerine karışması sebebiyle kınanmış ve karşı siber saldırlara maruz kalmıştır. Uluslararası arenada her zaman haklı olmak veya verilen tepkilere olumlu sonuçlar beklemek herkes tarafından kabul edilmemektedir.

Bunun en büyük örneği geçtiğimiz yıllarda Anonymous grubunun Türkiye'ye yapmış olduğu siber saldırı ve akabinde Türk hackerlar tarafından karşı saldırıya uğramasıdır. Şekil-6'da verilen görselde Anonymous grubunun Türk hackerlar tarafından hacklenmesi ve sistemlerinin devre dışı bırakılması gösterilmiştir. Anonplus bir zamanlar Anonymous sosyal ağı olarak kullanılmaktaydı.

Şekil-6: Türk hacker grubu tarafından Türkiye İç işlerine karışması sebebiyle hacklenen Anonymous grubu

Türk hacker grubunun Anonymous'u hacklemesi RF hükümeti ve RF yanlısı hacker gruplarının ülkelerine karşı yapılan siber saldırılara cevap verme olasılıklarını ve kendilerince haklı çerçevede yapacakları atakları göstermek için verilmiştir. Tüm bu araştırma ve bulgular neticesinde devlet destekli veya bağımsız hacker gruplarının RF-UK savaşında aktif olarak rol aldığı ve ulusal arenada etkili sonuçlarının olduğu görülmektedir.

Rus Hacker Grupları ve RF Kaynaklı Gerçekleşen Siber Saldırılar

Rusya-Ukrayna savaşı başladığından bu zamana kadar birçok teknoloji devi şirketleri ve araştırma ve raporlama şirketlerinin durumu yakından takip ettiği görülmektedir. Bu kapsamda siber saldırı boyutlarında hangi ülkenin ne kadar siber saldırı yaptığı veya ne kadar siber saldırı aldığı gibi konular gün yüzüne çıkarılmaktadır.

Microsoft'un Ukrayna'ya özel hazırlamış olduğu raporunda yaşanan siber etkinliğin detayları gözlemlenmektedir. Microsoft kurumsal başkan yardımcı Tom Burt yapmış olduğu bir analiz raporunda açıklamasında şu sözlere yer vermiştir: "İşgalden hemen önce başlayarak, Rusya ile uyumlu en az altı ayrı ulus-devlet aktörünün Ukrayna'ya karşı 237'den fazla operasyon başlattığını gördük - devam eden ve sivil refahı tehdit eden yıkıcı saldırılar

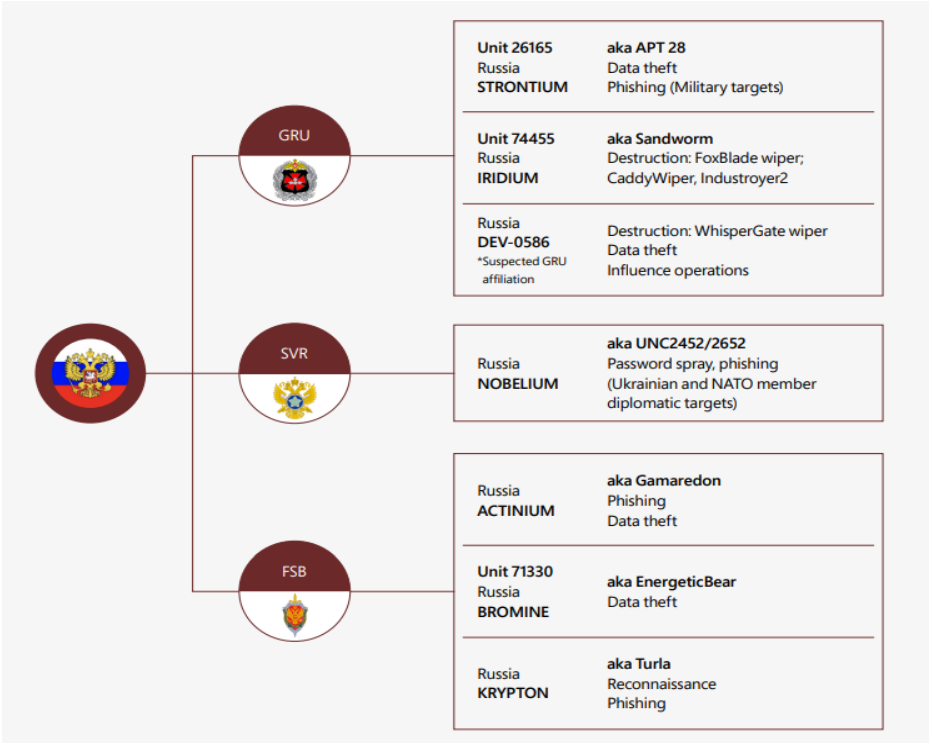
da bunlara dahildir. Yıkıcı saldırılara geniş çaplı casusluk ve istihbarat faaliyetleri de eşlik etti. Diğer NATO üye devletlerini içeren sınırlı casusluk saldırı faaliyeti ve bazı dezenformasyon faaliyetleri de gözlemledik (BleepingComputer, 2022).”

Rusya ile uyumlu tehdit gruplarının Mart 2021 gibi erken bir tarihte siber çatışma için ön konumlandırma yapması, yanı sıra geçmişte ara sıra Ukrayna'yı hedef alan tehdit aktörleri içindeki kuruluşlara karşı daha fazla eylem yapılmaya başlandığı gözlemlenmiştir. Yani geçmişten günümüze kadar düzenli olarak, sık sık olmasada Rus kaynaklı hacker gruplarının Ukrayna’ya saldırıları söz konusu olmuştur.

Rusya ile uyumlu hacker gruplarının, günümüzde Ukrayna’ya karşı yapılan siber saldırılarda rolü büyüktür. Bu hacker gruplarının bir kısmı aşağıda listelenmiştir ve çoğu RF devleti desteklidir.

- APT28
- Sandworm
- UNC2452/2652
- Gamaredon
- EnergeticBear
- Turla
- Conti Group

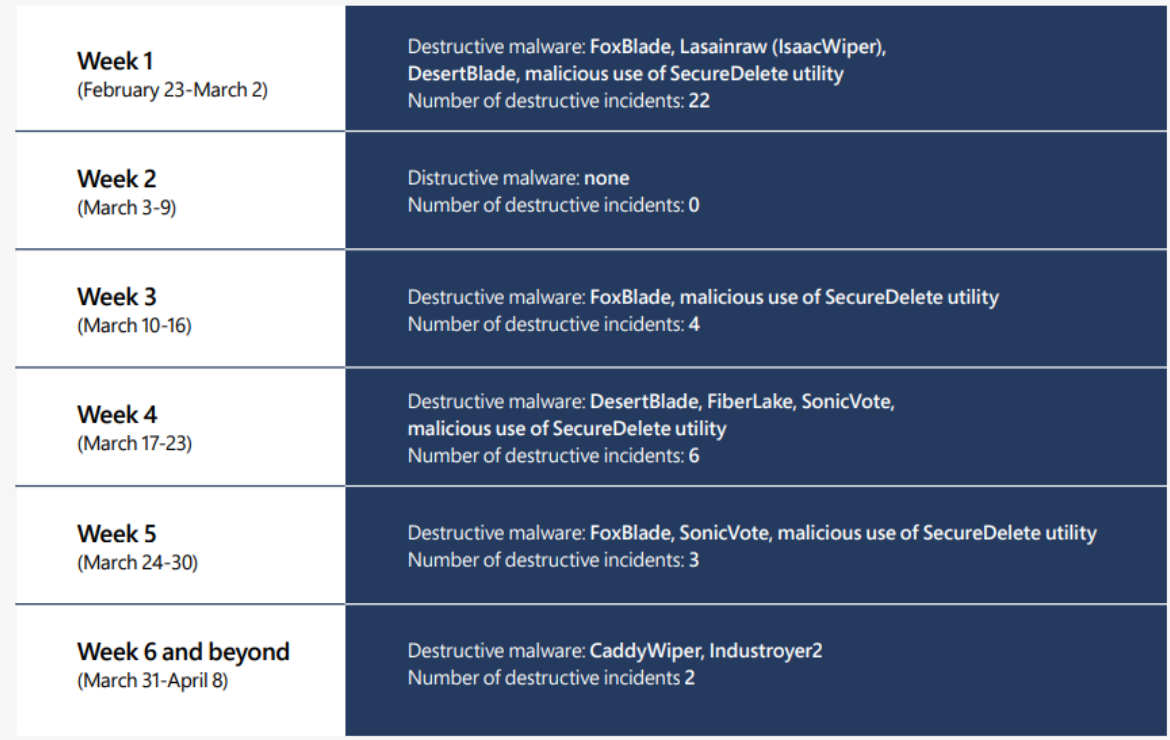
Aşağıda verilen şekilde (Şekil-7) RF taraflı hacker grupları ve Ukrayna tarafına yaptıkları siber saldırıların türleri verilmiştir. Aynı zamanda Rusya devleti organları tarafından desteklendiğine ve yönlendirme yapıldığına dair grafikselleştirmeye de yer verilmektedir.



Şekil-7: Rusya taraflı hacker grupları ve Ukrayna tarafına yaptıkları siber saldırıların türleri (Special Report: Ukranie – Microsoft, 2022)

Yukarıda listede yer alan grupların yapmış olduğu siber saldırılara bir örnek olarak NOBELIUM (UNC2452/2652 olarak da biliniyor) grubunun büyük ölçekli kimlik avı saldırısı başlatması ve bunu Rus birliklerinin fiziksel savaş bakımından Ukrayna'ya ilk ilerlemesi sırasında yapmış olması planlı ve sistematik bir siber saldırının gerçekleşmiş olduğunu kanıtlamaktadır. Yapılan kimlik avı saldırısıyla Ukrayna'nın askeri ve yabancı ortaklıkları hakkında istihbarat alınması hedeflenmesi ise yapılan siber saldırının derinliğini ve etkilerini göstermektedir.

Rusya devleti tarafından Ukrayna'ya gerçekleştirilen siber saldırıların yıkıcılık düzeyine göre listesi ve zararlı yazılım türleri Şekil-8'de gösterilmiştir (Special Report: Ukranie – Microsoft, 2022). Haftalık olarak değişen siber yıkım şiddetinin azalması, süreç içerisinde anlaşılmaya çalışan diplomatik meselelerin olması olarak yorumlanmaktadır. Yani diplomatik süreçlerde siber saldırıların kesildiği bulgusu ortaya çıkmaktadır.



Şekil-8: RF tarafından Ukrayna'ya gerçekleştirilen siber saldırıların yıkıcılık düzeyine göre haftalık listesi ve zararlı yazılım türleri

Rus askeri istihbarat teşkilatı GRU biriminin genellikle DDOS saldırılarını üstlendiği bir çok literatür tarafından doğrulanmaktadır. Bu hususta Şekil 7 de yer alan Rus birimlerinin çeşitli APT gruplarını ve kendi personellerini kullanarak siber saldırılar yapmakta olduğu gözlemlenmiş ve doğrulanmıştır.

Rusya destekli hacker grupları, Rus resmi birimleri ve Ukrayna tarafına yapılan siber saldırılar ele alındığında ve detaylı olarak incelendiğinde saldırıların halen devam etmekte olduğu ve çeşitli yöntemler kullanılarak Ukrayna tarafına ciddi oranda siber saldırılar gerçekleştiği görülmektedir. Bir diğer hususta bu siber saldırıların ve Rus destekli hacker

gruplarının güç dengesinde bir hayli etkili olabileceği de yaşanan Rusya-Ukrayna savaşında ispat edilmiş/edilmektedir.

UK Hacker Grupları ve UK Kaynaklı Gerçekleşen Siber Saldırılar

Rusya-Ukrayna savaşının resmi olarak başlamasından günümüze kadar Ukrayna tarafına dünya genelinde siber anlamda birçok destek gelmiştir. Bunlar arasında resmi hacker grupları olduğu gibi hacktivist eylemlerde bulunan gruplar da yer almaktadır. Ukrayna devletinin resmi hacker grubu oluşturduğu ve resmi birimlerince bu gruba destek verdiği ve halka açık biçimde eylemlerde bulunduğundan bahsetmiştik.

Bu hususta IT Army of Ukraine Ukrayna tarafında en önde gelen resmi siber saldırı gruplarının başını çekmektedir. Bunun dışında resmi olmayan hacker grupları da vardır. Ukrayna destekli gruplar aşağıda liste olarak verilmiştir.

- IT Army of Ukraine
- Anonymous
- Belarusian Cyber Partisans
- GhostSec
- ContiLeaks

IT Army of Ukranie grubuna doğrudan destek veren ve bir siber ordu oluşturulmasında etkin rol oynayan hacker grupları kendi içlerinde belirledikleri organizasyonlar neticesinde de Rusya tarafına siber ataklar gerçekleştirmektedir. Fakat gözlemler ve bulgular neticesinde IT Army of Ukranie grubunun tek bir çatı görevi görmesi, Ukrayna açısından siber alanda ciddi prestij ve başarılı sonuçlar alınmasını beraberinde getirmiştir.

Tüm bu resmi ve hacktivist gruplar dışında, devletlerin siber birimlerinin doğrudan Ukrayna tarafına destek vermesi söz konusudur. Şöyle ki Rusya'ya savaşı başlatması gerekçesiyle tüm dünya tarafından uygulanan yaptırımlar arasında siber alanda yapılan yaptırımlar da söz konusu olmaktadır. Dolayısıyla Rusya tarafına dünya genelinde yapılacak bir siber yaptırımın Ukrayna tarafına destek olacağı görülmektedir.

Bu konuda en büyük örnek ABD'nin açıklamalarıdır. Şekil-9'da bir haber kaynağından alınan paragrafa yer verilmiştir. Alıntıda ABD'nin Rusya tarafına yapacağı siber saldırı seçenekleri görülmektedir.

> Seçenekler arasında, Rusya genelinde internet bağlantısını kesmek, elektriği kesmek ve Rusya'nın ikmal kabiliyetini engellemek için demiryolu makaslarını kurcalamak yer aldı.
>
> Kaynaklardan biri, "Bu sayede trenleri yavaşlatmaktan raydan çıkmalarını sağlamaya kadar, her şeyi yapabilirsiniz" dedi.
>
> ABD Siber Komutanlığı, Ulusal Güvenlik Ajansı, CIA ve diğer kurumların olası operasyonlarda rol oynayacağı düşünülüyor.
>
> NBC ayrıca, bu olası eylemlerin, Rusya'nın Ukrayna'yı işgaline karşı önleyici yanıtlar olarak düşünüldüğünü bildirdi.

Şekil-9: ABD tarafından Rusya'ya yapılacak gerçekleşmemiş siber yaptırım senaryoları (Independet Türkçe, 2022)

UK taraflı saldırıların çeşitlerine bakıldığı zaman, genellikle erişimi kesme, yani DDOS saldırılarının yüksek oranda olduğu görülmektedir. Bunun yanında ransomware tarzı saldırıların da etkisi görülmektedir. Örneğin "RURansom Wiper Targets" isminde ortaya çıkan zararlı yazılım hedefte bulunun kritik dosyaları direkt silebilme özelliğine sahip olduğu gözlemleniyor. Etkin hedefler olmasada birkaç hedef üzerinde bu zararlı yazılım ile siber saldırılar gerçekleştiği görülmektedir.

Bu ransomware türü yazılımın diğerlerinden farkı fidye istemeden veya tehdit unsuru oluşturarak sistemi kitlemeden direkt hedefe odaklanıp hedefteki dosyaları yok etmeye programlanmış olmasıdır. Siber savaşta görülebilecek yazılım türlerinden olduğu gibi fidye ihtiyacını da ortadan kaldırmaktadır.

Şekil-10'da verilen görselde RURansom zararlısının yazılımcısı tarafından verilen mesaj yer almaktadır. Genellikle zararlı yazılım mesajı not (şifreleme ve yok etme sonrası metin belgesi bırakarak) şeklinde ekranda görülmesini sağlamaktadır.

```
string[] contents2 = new string[] { "24 февраля президент Владимир Путин объявил войну Украине.", "Чтобы
противостоять этому, я, создатель RU_Ransom, создал эту вредоносную программу для нанесения ущерба России. Вы
купили это себе, господин президент.", "Нет никакого способа расшифровать ваши файлы. Никакой оплаты, только
ущерб. И да, это \"миротворчество\", как это делает Влади Папа, убивая невинных мирных жителей", "И да, это
было переведено с бангла на русский с помощью Google Translate..." };
```

Şekil-10: RURansom geliştiricisi tarafından zararlı yazılım içerisinde Rusya'ya verilen mesaj ve zararlı yazılımın amacını gösterir ifadeler

Notun İngilizce versiyonu kaynaklarca şu şekilde çevrilmiş. "24 Şubat'ta Başkan Vladimir Putin Ukrayna'ya savaş ilan etti.", "Buna karşı koymak için, RU_Ransom'un yaratıcısı ben, Rusya'ya zarar vermek için bu kötü amaçlı yazılımı yarattım. Bunu kendiniz için aldınız Sayın Başkan.", "Dosyalarınızın şifresini çözmenin bir yolu yok. Ödeme yok, sadece hasar. Ve evet, bu Vladi Papa'nın yaptığı gibi "barışı koruma", masum sivilleri öldürme", "Ve evet, Google Translate kullanılarak Bangla'dan Rusça'ya çevrildi..." (TrendMicro, 2022)

Şekil-11'de zararlı yazılımın son aşamalarından şifreleme anahtarı oluşturmanın kod analizleri verilmiştir. Sunucuya erişim sağlanır ve şifreleme oluşturulur detaylar şifreleme anahtarı oluşturma ile gösterilmiştir.

```
// Token: 0x0600000A RID: 10 RVA: 0x00002554 File Offset: 0x00000754
private static string[] getEncryptedAesKey()
{
    AesCrypter aesCrypter = new AesCrypter();
    byte[] bytes = Encoding.UTF8.GetBytes(Program.BuildPassword("FullScaleCyberInvasion + " + Environment.MachineName));
    byte[] bytes2 = Encoding.UTF8.GetBytes(Program.BuildPassword("RU_Ransom" + Environment.UserName + "2022"));
    byte[] inArray = AesCrypter.AES_Encrypt(bytes, bytes2);
    return new string[]
    {
        Convert.ToBase64String(bytes),
        Convert.ToBase64String(bytes2),
        Convert.ToBase64String(inArray)
    };
}
```

```
// Token: 0x0600000B RID: 11 RVA: 0x000025E0 File Offset: 0x000007E0
private static string BuildPassword(string str)
{
    StringBuilder stringBuilder = new StringBuilder();
    Random random = new Random();
    for (int i = 0; i < str.Length; i++)
    {
        stringBuilder.Append(str[random.Next(0, str.Length)]);
    }
    return stringBuilder.ToString();
}
```

Şekil-11: RURansom şifreleme anahtarı oluşturma

RURansom yazılımının sürekli güncellendiği ve yeni sürümlerinin yayınlandığı da tehdit raporlarında gözlemlenmektedir. Aktif devam eden savaş sürecinde siber alanda kullanılmaya devam eden RURansom yazılımı UK taraflı ransomware türü saldırıların en büyük örneği olarak gösterilebilir ve Rusya tarafını kızdıracak derecede zarar verme potansiyeli olduğu gözlemlenmiştir.

SONUÇ, TARTIŞMA VE ÖNERİLER

Sonuç

Bu çalışmada Rusya ve Ukrayna arasında yaşanan gerilimin savaşa dönmesinden sonra siber alanda yaşanan gelişmeler önce dünya genelinde özetlenmiş ve daha sonra RF-UK savaşı bağlamında siber güvenlik ekosisteminde öne çıkan gelişmeler aktarılmıştır.

Savaştan günümüze kadar siber alanda çeşitli aksiyonlara şahit olunmuştur. Bunlar olabildiğince net özetlenerek literatür dışına çıkılmamıştır. Siber alanın gerektirdiği konular RF-UK savaşı bağlamında özetlenerek: yapılan siber saldırılar, zafiyetler, önlemler, kurum ve kuruluşların gördüğü zararlar her iki ülke açısından yaşanan siber kayıplara araştırmamızda ışık tutulmaktadır.

Tüm bu çalışma literatür taramasında basılı kaynaklar ve internet yayınları, raporlar ve makaleler aracılığı ile toparlanmıştır.

Tartışma

Araştırmanın önemli istatistiksel sonuçlarından birisi dünya genelinde siber saldırı kavramının yıkıcı tahriplere yol açması ve fiziksel savaştan öte sonuçlara gebe olması olarak gösterildiğinde siber savaş ve siber uzay olgularının önemi üzerinde farkındalık oluşturulması gerektiği gözlemlenecektir. Ve olası sonuçlar tekrar gözden geçirilmelidir.

Öneriler

Yaşanan siber savaşın yıkıcı tarafları incelenerek her ülkenin kendi savunma stratejilerini oluşturması söz konusu olabilmektedir. Tarihte resmi olarak ilk siber savaş olma özelliği RF-UK savaşında görülmüştür. Bu hususta yapılan gayriresmi siber savaşlar da incelenerek uluslarası hukuk boyutları ele alınabilir ve bu konuda yeni bir proje/tez yazılabilir. Sonuç son yıllarda gelişen siber ataklar ve savunma stratejileri bu savaş üzerinden yorumlanabilir ve geliştirilebilir.

KAYNAKÇA

[1] İnternet: T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2019). Ulusal Siber Güvenlik Stratejisi , Sf: 7 Web: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf adresinden alınmıştır.

[2] Bayraktar, G. (2015). Siber Savaş ve Ulusal Güvenlik Stratejisi (Birinci Baskı). Türkiye: Yeniyüzyıl Yayınları, 48-49.

[3] İnternet: Bilişim İnovasyon Derneği, (2021). Siber Güvenlik Raporu, Sf: 9 Web: http://www.bilisiminovasyon.org.tr/webfiles/userfiles/files/siber_guvenlik_raporu.pdf adresinden alınmıştır.

[4] İnternet: TUBİTAK BİLGEM, (2022). Rusya-Ukrayna Siber Savaş Tehdit Araştırma Raporu, Sf: 1-5 Web: https://bilgem.tubitak.gov.tr/sites/images/tubitak_bilgem_sge_rusya-ukrayna_siber_savas_tehdit_arastirma_raporu.pdf adresinden alınmıştır.

[5] Singer, P.W., Friedman, A. (2018). Siber Güvenlik ve Siber Savaş (İkinci Baskı). Türkiye: Buzdağı Yayınları, 24-26.

[6] İnternet: CyberMag, (2022). Rusya ve Ukrayna Arasındaki Siber Savaş Dünyayı Derinden Etkiliyor, Web: https://www.cybermagonline.com/rusya-ve-ukrayna-arasindaki-siber-savas-dunyayi-derinden-etkiliyor adresinden alınmıştır.

[7] İnternet: BleepingComputer, (2022). Microsoft says Russia hit Ukraine with hundreds of cyberattacks, Web: https://www.bleepingcomputer.com/news/security/microsoft-says-russia-hit-ukraine-with-hundreds-of-cyberattacks/ adresinden alınmıştır.

[8] İnternet: Microsoft, (2022). Special Report: Ukraine - An overview of Russia's cyberattack activity in Ukraine, Web: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd adresinden alınmıştır.

[9] İnternet: Independet Türkçe, (2022). Cephe gerisinde kıran kırana mücadele: Örneklerle Rusya - Ukrayna siber savaşı, Web:

https://www.independentturkish.com/node/481006/d%C3%BCnya/cephe-gerisinde-k%C4%B1ran-k%C4%B1rana-m%C3%BCcadele-%C3%B6rneklerle-rusya-ukrayna-siber-sava%C5%9F%C4%B1 adresinden alınmıştır.

[10] İnternet: TrendMicro, (2022). New RURansom Wiper Targets Russia, Web: https://www.trendmicro.com/en_us/research/22/c/new-ruransom-wiper-targets-russia.html adresinden alınmıştır.