29.06.2022

ISIM: Altay Yücetas

UNIVERSITE/BOLUM: ODTU/Bilgisayar Mühendisligi

Cyber Threat Intelligence

İÇİNDEKİLER

Önde Gelen Hacker Forumları

1- **Reddit:** Reddit aslında hacking üzerine kurulmuş bir sosyal medya ortamı değil. Reddit, içerisinde binlerce subreddit (kullanıcıların belirli bir alanda paylaşım yaptığı forumsal başlıklar) barındıran bir oluşum. Ve kullanıcılar istedikleri alanda subreddit açmakta özgürler. Tabii ki de bu subredditlerin bazıları da hacking, phishing, social engineeing alanlarında oluyor. Bu alanlarda önde gelen subredditler genellikle "etik" başlığından uzaklaşmaktan kaçınıyorlar. Fakat yeni açılmış veya az üyesi bulunan subredditlerde kullanıcı konularındaki kontrol mekanizması çok gelişmiş olmadığından suç sayılabilecek konulara sıkça rastlamak mümkün. Bu subredditler yasalara ve Reddit'in kendi kurallarına karşı geldiğinden kapatılabiliyorlar.

2- **0x00sec:** 0x00sec sadece hacking tabanlı olan ve en kalabalık forumlardan bir tanesi. Bug Bount'den Hardware Hacking'e kadar geniş çaplı kategoriler sunan bu site genel olarak "etik" kavramının dışına çıkmıyor. Bundan dolayı bu siteye "etik hacker'ların evi" de denebilir.

HACK FORUMS

3- **Hack Forums:** Hack Forums da aynı oxoosec gibi sadece hacking tabanlı olan kalabalık forumlardan bir tanesi. Site genel olarak eğitsel materyaller ve hacking alanında kullanılabilecek toollar sunuyor. Başlangıç ve ileri düzey kullanıcılar için ayrı kategoriler oluşturulmuş. Yani kullanıcılar başlangıç kategorisinde onlardan daha deneyimli kullanıcılara soru sorabiliyor. Ayrıca, bunların dışında garip bir alt kategori bulunduruyor, "Request For Hacking". Kullanıcılar, bu alt kategoride diğer üyelerden bir sitenin gizli verilerini bulmalarını veya bir sosyal medya hesabını ele geçirmelerini isteyebiliyor. Bu alt kategori hiçbir şekilde yasal bir geçerliliğe bağlı olmamasına rağmen site üzerinde garip bir şekilde varlığını sürdürüyor.

4- **Turk Hack Team:** Hacking alanındaki başka bir site ise Turk Hack Team. Bu sitenin göze çarpan özelliklerinden en önemlisi bunun bir Türk sitesi olması. Bunun yanında eski ve köklü bir site olması bu sitenin tanınır ve içerik bakımından zengin olduğu anlamına geliyor. Bu site sadece hacking alanında değil oyunlardan e-ticarete kadar birçok alanda içerik bulunduran bir forum. Site genel olarak yasa dışı bir içerik bulundurmuyor fakat "THT Gövde Gösterisi" kısmında kullanıcılar ele geçirdikleri siteleri ve o siteye ait verileri yayınlayabiliyorlar. Ama site adminin bu ayın başında yaptığı bir açıklama ile bu kategori artık kullanılamıyor.

5- **Crax.Pro:** Crax.Pro, daha çok siyah şapkalı hacker'ların kullandığı bir forum. Bu site genel olarak yasa dışı konular içermekte ve site kullanıcılarının insanları dolandırarak elde ettikleri kredi kartı bilgilerinin paylaşımı yapılmaktadır. Aynı zamanda kullanıcılar, gerçek kişilere ait olan kredi kartı bilgilerini kullanırken nasıl yakalanmayacakları konusunda da birbirlerine tavsiyeler veriyor. Bunların dışında kullanıcılar, ele geçirdikleri sitelerin veri tabanlarını da bu site üzerinden satıyor/yayınlıyorlar.

6- **CrdForum:** Bu site aslında yukarıdakiler kadar büyük ve geniş bir kitleye hitap eden bir forum değil. Hatta yeni bile açılmış denebilir. Crax.Pro gibi siyah şapkalı hacker'lara hitap ediyor ve yasa dışı konular içeriyor. Bu forumu buraya koymamdaki asıl sebep özel olarak "Fraud Education" adında bir kategori içermesi. Bu kategori ve bu kategorinin alt kategorilerinde kullanıcılar, diğer kullanıcılara nasıl dolandırıcılık yapabilecekleri konusunda tavsiyeler veriyor.

Kategorilendirme

Bu başlık altında yukarı bahsettiğim siteleri ve daha fazlasını içerdiği içeriklere, kullanıcıların kullanım amacına ve yasalara uygunluğu açısından kategorilendireceğim.

Forumları ilk olarak yasal olup olmamaları açısından sınıflandıracağım. Yasalara uygunluk konusunda sınıflandırma kriterim sadece bu alanda içerik içermesi değil, aynı zamanda site yöneticilerinin ve moderatörlerin bu içeriklere ne denli izin verdiği ile ilgili de olacaktır.

Yasalara Uygun	Yasalara Yarı Uygun	Yasa Dışı
1- Reddit	1- Turk Hack Team	1- CrdForum
2- 0x00sec	2- Cracking	2- Crax.Pro
3- Malvult	3- Level23hacktools	3- Altenen
4- Kernel Mode	4- Eleaks	4- CardingForum
5- BHF.IM	5- SpyHackerz	5- DarkNetWeb
6- GreySec		6- Nulled
7- Malwaretips		
8- AntiOnline		
9- Wilders Security		

Forumları sınıflandırmada kullanacağım diğer bir parametre onların içeriği hakkında olacaktır. Bazı forumlar "carding" olarak adlandırılan kredi kartı dolandırıcılığını gibi yasa dışı eylemleri ön plande tutarken bazıları da eğitsel içeriklere daha çok önem veriyor. Bunları baz alarak bir sınıflandırma yapacağım.

Dolandırıcılık

1- Crax.Pro
2- CrdForum
3- CardingForum
4- DarknetWeb

Çeşitli

1- Altenen
2- Cracking
3- HackingFather
4- Turk Hack Team
5- SpyHackerz
6- AntiChat

Eğitim

1- Reddit
2- 0x00sec
3- HackForums
4- GreySec
5- Malvult
6- KernelMode

Sızıntı Veri

1- Level23HackTools
2- Eleaks
3- Nulled

İstihbarat Türleri

Hacker'lar, kullandıkları forumlar üzerinden bilgi ve veri paylaşımı yapabilirler. Bunlar 0-day zafiyetlerden kendi yapımları malware'lere kadar her şey olabilir. Ve bu bilgi ve veriler istihbarat açısından çok büyük değer taşır. Siber Tehdit İstihbaratı alanında çalışan kişiler bu verileri kullanarak bunlara karşı savunma ve çözüm sistemleri geliştirebilirler. Siber Tehdit İstihbaratı alanında çalışanlar kişilerin bu forumlarda toplayacağı birkaç tür veri vardır. Bunlardan bazıları şu şekilde sıralanabilir:

1- Malware Intelligence: Kullanıcılar, forumlardan kendi yaptıkları veya başkaları tarafından yapılıp GitHub gibi platformlara konulan malware'leri paylaşabilirler. Bu malware'ler ve onların nasıl çalıştıkları konusunda bilgiler elde etmek hem onlar hem de onların benzerleri için bir savunma sistemi inşa etmeye olanak tanır. Aynı zamanda bu istihbarat türü, APT gruplarının kullandıkları malware'ler için de elde edilirse bu APT gruplarının nasıl çalıştıkları ve hangi sektörleri hedeflemek istedikleri de anlaşılabilir.

> Title says it all what are the best rats in 2022 paid or free.
> Functions that i need the most are keylogger and password recovery.
> Tnx

Örnek olarak forumlardan bir tanesinde kullanıcı 2022 yılında sunulan RAT (Remote Access Trojan) tipindeki malware'lerden en iyi nedir diye sormuş.

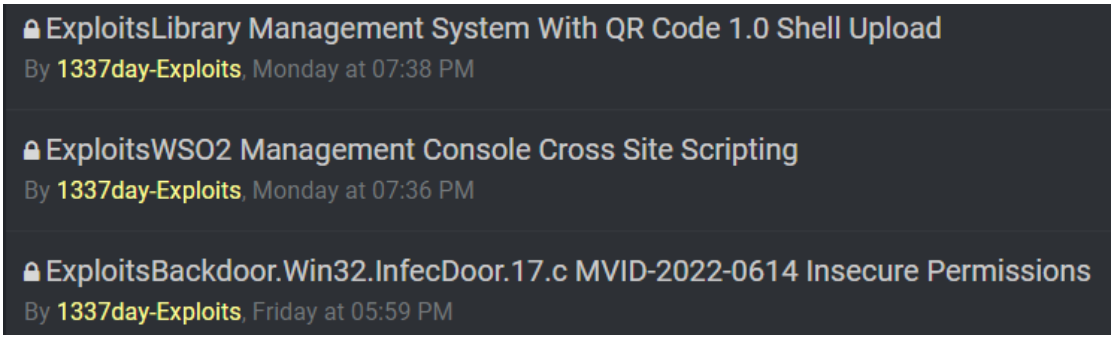
> Quasar, Async, and DcRAT are some free ones to name.

> hello,
> free rat Quasar or dcat nice tools

Başka kullanıcılar da soruyu soran kullanıcıya birkaç RAT tipindeki malware'leri önermişler. Bu RAT'ler elde edilebilirse tersine mühendislik ile içeriği hakkında daha fazla bilgiler elde edilebilir.

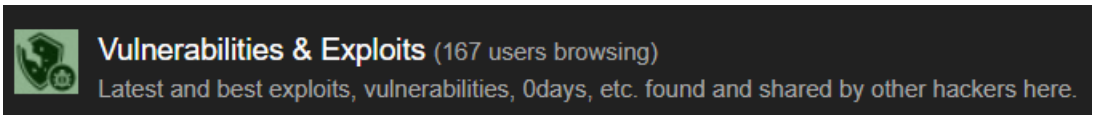
2- **Exploit Intelligence:** Exploit'ler sistem üzerinde bulunan bir zafiyeti kullanarak sisteme kendi istekleri şeyi yaptırmak için yazılmış kod parçalarıdır. Ve bu zafiyet, 0-day bir zafiyet ise o zaman sistemde ciddi hasarlara yol açabilir. Bu tür zafiyetleri istismar etmek için zafiyete özel exploit oluşturan kişiler oluşturdukları dosyayı forum sitelerinde yayınlayabilirler. Bunun nedeni kendilerini ispatlamak veya dünyanın her tarafındaki cihazlarda bu zafiyetin istismar edildiğini görme hırsı olabilir. Forumlardan elde edilen bilgiler hem zafiyetin daha kısa sürede kapatılmasına hem de bu zafiyete karşı aktif bir savunma sistemi geliştirilmesine olanak tanır.

Forumlarda, aşağıdaki resimde de görüldüğü gibi exploit paylaşımları yapılabilmektedir.

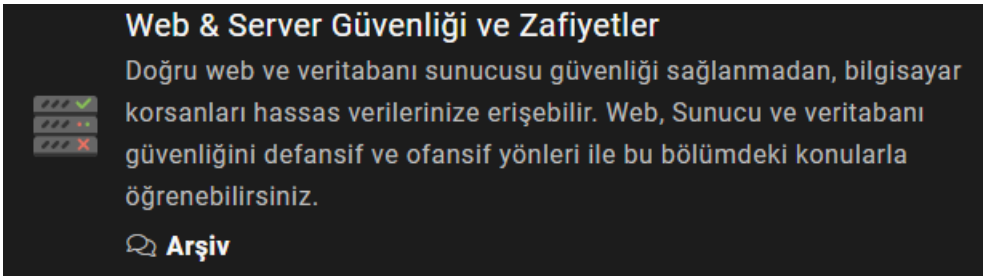


3- **Vulnerability Intelligence:** Forumlarda, exploit istihbaratından farklı olarak sadece sistem üzerindeki zafiyetler hakkında da bilgi edinilebilir. 0-day bir zafiyet hakkında konu paylaşılmışsa yukarıda da bahsedildiği gibi zafiyeti erkenden farkedip kapatmak hem gelecekteki olası saldırıların önüne geçer hem de halihazırda sisteme sızmış saldırganların sistemden çıktıklarında geri dönememelerini sağlayabilir. Bu yüzden bu forumlardan elde edilen zafiyet (vulnerability) istihbaratı ölümcül derecede önemli olabilir.

Aşağıda bir hacking forumunda oluşturulmuş ve zafiyetleri de içeren bir kategori görülüyor.

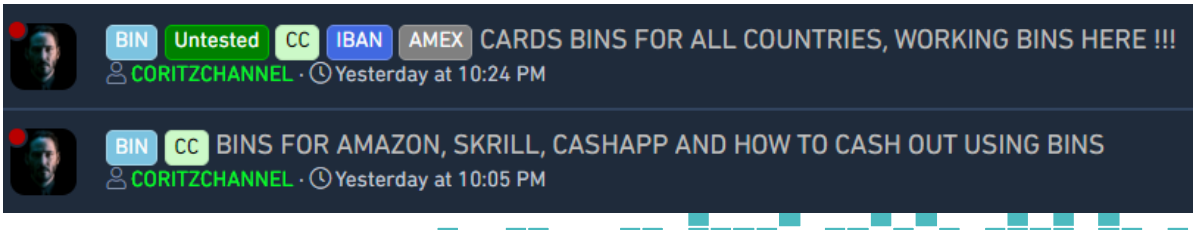


Aşağıdaki görsel bir Türk forumundan alındı.



4- Cyber Crime Intelligence: Raporun başında hacking alanındaki forumlar hakkında yazı yazarken bazı forumların dolandırıcılar için oluşturulmuş olduğunu ve burada paylaşılan konular için yasalara uygunluğu açısından neredeyse hiçbir kontrol mekanizması olmadığından bahsetmiştim. Bu forumlardan elde edilebilecek suçlar hakkındaki istihbarat birden çok fayda sağlayabilir. İlk olarak bu suçların genellikle hangi sektörleri hedeflediği belirlenebilir. Forumlarda paylaşılan içerikler genellikle belirli bir şirkete (genellikle dünya çapındaki büyük şirketlere) ait olan ve bu şirketlerin veri tabanlarının veya özel bilgilerinin ele geçirilmesiyle oluşmuş bilgilerden oluşur. Sızdırılan bilgilerden ve saldırıya uğramış şirketlerin bulunduğu sektörleri sınıflandırarak hangi sektöre ne kadar saldırı yapıldığı, bu saldırıların motivasyon kaynağının en çok ne olduğu, saldırganların saldırıdan sonra bu verileri ne yaptıkları gibi istihbaratlar elde edilebilir.

Aşağıda da görüldüğü gibi forumlarda, büyük şirketler üzerinden dolandırıcılık yapmak amacıyla açılmış konular görülüyor.

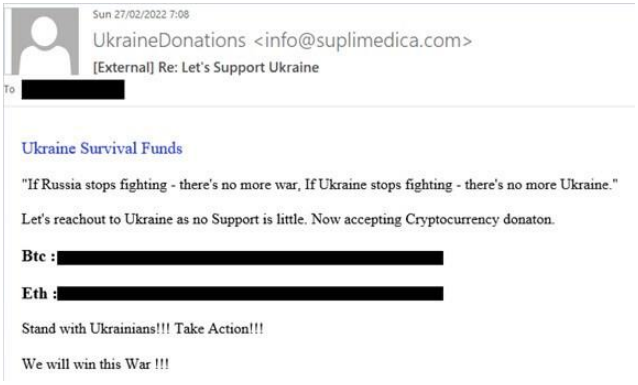


Güncel Dolandırıcılık Yöntemleri

Uzun zamandır uygulanan dolandırıcılık yöntemleri artık bu yöntemler için özel olarak hazırlanan yazılımlar ve yapay zekanın yardımı ile yavaş yavaş yok olmaya başlıyor. Fakat dolandırıcılar da yeni teknikler keşfetmekten vazgeçmiyor. Bu tekniklerin de herkes tarafından bilinmesi ve bunlara karşı önlem alınması çok önemli. Bu başlık altında son zamanlara ortaya çıkan dolandırıcılık tekniklerini sıralayıp onlar hakkında birkaç şey yazacağım.

1- Ukrayna Savaşı: Bilindiği gibi 2022 yılının Şubat ayında Rusya, Ukrayna'yı işgal etti. Ve dünyanın her tarafındaki insanlar Ukrayna'ya destek olmak için her şekilde bağış yapmak istediler. Dolandırıcıların kullandığı teknik de bunun üzerine kuruldu. Dolandırıcılar, insanların mail adreslerine "Ukrayna'ya yardım etmek ister misiniz?" şeklindeki mailler atmaya başladı ve konunun içeriğinde bağış yapmak isteyenler için kendi Bitcoin ve Etherium cüzdanlarının numaralarını verdiler. Bu maili alan yardımsever vatandaşlar da maili gerçek zannedip o hesaplara paralarını gönderdiler. Ne kadar bilinçli kullanıcılar bu yönteme kanmamış olsalar da saf kişiler paralarını dolandırıcılara kaptırdı. Bu savaşı baz alan başka bir dolandırıcılık yöntemi ise bundan daha tehlikeliydi. Saldırganlar anketör kılığına girerek tedarikçilere bu savaştan dolayı nasıl bir back-up planları olduklarını sormak amacıyla bir mail gönderdiler. Bu mail zararlı bir yazılımdan oluşan bir dosya içeriyor. Tedarikçinin bu ankete yanıt verebilmesi için ilk olarak maildeki dosyayı indirmesi gerekiyor. Tabii ki indirdikten sonra çok geç oluyor. Dolandırıcı, şirketin özel dosyalarını ve veri tabanını forumlarda satışa sunuyor. Bu gibi yöntemler dolandırıcıların bu yılki kullandığı kandırma teniklerinden birkaç tanesi.

Aşağıda, Ukrayna Savaşı'nı kullanarak insanları dolandırmaya çalışan bir dolandırıcı görülüyor.


Sun 27/02/2022 7:08

UkraineDonations <info@suplimedica.com>

[External] Re: Let's Support Ukraine

To [redacted]

Ukraine Survival Funds

"If Russia stops fighting - there's no more war, If Ukraine stops fighting - there's no more Ukraine."

Let's reachout to Ukraine as no Support is little. Now accepting Cryptocurrency donaton.

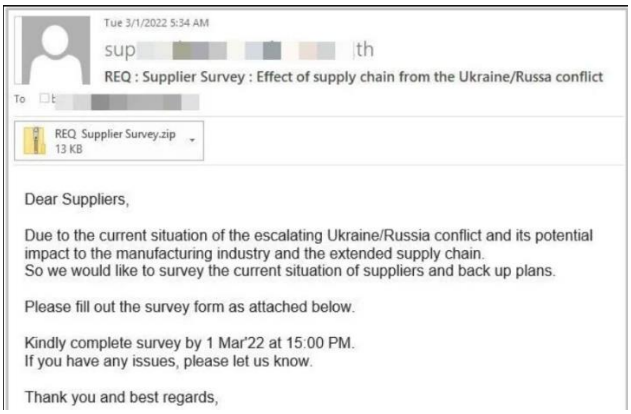
Btc : [redacted]

Eth : [redacted]

Stand with Ukrainians!!! Take Action!!!

We will win this War !!!

Aşağıda ise tedarikçileri kandırmaya çalışan bir dolandırıcı görülüyor.


Tue 3/1/2022 5:34 AM

sup [redacted] th

REQ : Supplier Survey : Effect of supply chain from the Ukraine/Russa conflict

To [redacted]

REQ Supplier Survey.zip
13 KB

Dear Suppliers,

Due to the current situation of the escalating Ukraine/Russia conflict and its potential impact to the manufacturing industry and the extended supply chain.
So we would like to survey the current situation of suppliers and back up plans.

Please fill out the survey form as attached below.

Kindly complete survey by 1 Mar'22 at 15:00 PM.
If you have any issues, please let us know.

Thank you and best regards,

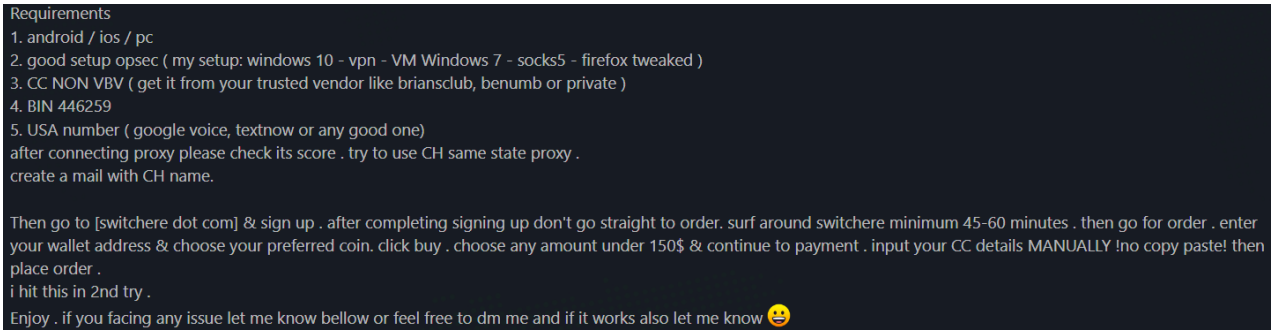
2- BIN BruteForce: Bu metod aslında yeni değil, birkaç yıldan beri kullanılıyor. Fakat son yıllarda CPU ve GPU'ların gücünün artmasından dolayı bruteforce saldırıları daha da kolaylaştı. Dolandırıcılar da bunun gibi methodları son zamanlarda daha sık kullanmaya başladı. Kredi kartı numarasının ilk 6 rakamı BIN (Bank Identification Number) olarak bilinir ve bu rakam kartını yayınlayan bankaya özeldir. Bunun bilen bir dolandırıcı, kendisinin bildiği 6 haneli bir sayıya sahip olan bankanın müşterilerine saldırmayı seçebilir. Bir yazılım ile bütün olası kart numaralarını üretmeye çalışır. Ayrıca bunlar için bir de CVV ve son kullanım tarihi de üretmesi gerekir. Bu ürettiği kart numaralarının gerçek olup olmadığını anlamak için ile düşük ücretli satın alımlar yapmaya başlar. Eğer satın alım sistemi herhangi bir uyarı vermezse demek ki kart numarası doğru tahmin edilmiş demektir. Dolandırıcı

eğer gerçek bir kart bulursa bu sefer büyük ücretli satın alımlar yapar ve kartın bakiyesi tükenene kadar harcamaya devam eder.

Aşağıdaki görsel basit bir biçimde saldırıyı açıklıyor.

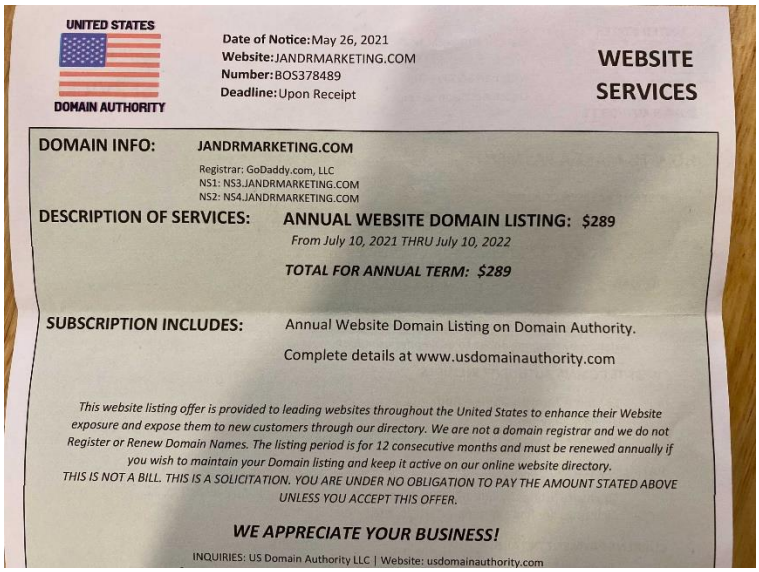
BIN/IIN	Bruteforce	Last 4
4329 95	XX XXXX	1234

Ayrıca dolandırıcılar, elde ettikleri bu kart verilerini nasıl kullanacakları hakkında forumlardan bilgi elde edebiliyor. Aşağıda da buna örnek bir görsel var.



3- US Domain Authority: Bu tekniğe aslında yarı dolandırıcılık tekniği diyebiliriz. Öncelikle bu yarı(!) dolandırıcılık tekniği Amerika'da geçerli olan bir teknik. Bir iş yeri sahibiyseniz ve bir websiteniz var ise "US Domain Authority"den gelen bir mektup alıyorsunuz. Mektup size yıllık domain listeme ücreti olarak 289 doları ödemelisiniz diyor. Ayrıyeten mektubun sol üst tarafında Amerika'nın bayrağı ile birlikte "US Domain Authority" de yazması dolandırıcıların Amerika Birleşik Devlet'lerinin resmi bir kurumu olduğu izlenimi uyandırıyor. Fakat bu site aslında herhangi bir resmi kuruma ait değil. Sitelerine girildiği taktirde bu ücretin aslında onların sitesindeki domain listeleme ücreti olduğunu anlıyorsunuz. Ve sitelerinde de bu ücreti ödemek zorunlu değildir diyor. Yani bu site, iş yerlerinin domain adreslerini, dolandırıcıların kendi sitesinde yayınlamak için ücret istiyor. Aslında bu yasal bir şey fakat bunu "US Domain Authority" ismi altında

yapmaları onları dolandırıcı kategorisi altına sokuyor çünkü dikkatsiz kullanıcılar bunun resmi bir belge olduğunu zannedip ödeme yapabilirler. Aşağıda da bu belgenin görsel hali var.



UNITED STATES
DOMAIN AUTHORITY

Date of Notice: May 26, 2021
Website: JANDRMARKETING.COM
Number: BOS378489
Deadline: Upon Receipt

WEBSITE SERVICES

DOMAIN INFO: JANDRMARKETING.COM
Registrar: GoDaddy.com, LLC
NS1: NS3.JANDRMARKETING.COM
NS2: NS4.JANDRMARKETING.COM

DESCRIPTION OF SERVICES: **ANNUAL WEBSITE DOMAIN LISTING: $289**
From July 10, 2021 THRU July 10, 2022
TOTAL FOR ANNUAL TERM: $289

SUBSCRIPTION INCLUDES: Annual Website Domain Listing on Domain Authority.
Complete details at www.usdomainauthority.com

This website listing offer is provided to leading websites throughout the United States to enhance their Website exposure and expose them to new customers through our directory. We are not a domain registrar and we do not Register or Renew Domain Names. The listing period is for 12 consecutive months and must be renewed annually if you wish to maintain your Domain listing and keep it active on our online website directory.
THIS IS NOT A BILL. THIS IS A SOLICITATION. YOU ARE UNDER NO OBLIGATION TO PAY THE AMOUNT STATED ABOVE UNLESS YOU ACCEPT THIS OFFER.

WE APPRECIATE YOUR BUSINESS!

INQUIRIES: US Domain Authority LLC | Website: usdomainauthority.com

Hedef Alınan Sektörler

Yukarıda da bahsedildiği üzere hacker forumlarında onlarca kişi, şirket ve sektör hedef alınıyor. İnsanlardan dolandırıcılık yöntemi ile, şirket ve sektörlerden ise sızdırdıkları veriler ile kazanç sağlıyorlar. Aynı zamanda dolandırdıkları insanların bilgilerini kullanarak şirketler ile ticaret yapabiliyor ve her iki tarafı da aynı anda zarara uğratabiliyorlar.

Saldırganların sıklıkla saldırdıkları ve dolandırdıkları şirket ve sektörleri eğer sıralayacak olursak en başta e-ticaret siteleri gelir. Saldırganlar, kişileri dolandırarak ele geçirdikleri kart bilgilerini e-ticaret sitelerinden ürün almak için kullanıyorlar. Bu çalıntı kartlarla yapılan alışverişler, kartı çalınan kullanıcının bildirmesi üzerine daha sonra iptal ediliyor fakat e-ticaret siteleri çalıntı kart ile satın alınan ürünü çoktan gönderdiği için zarar girmiş oluyor. Ama bu yöntem, saldırganın kendisinin veya bir tanıdığının ev adresini vermesini gerektirdiğinden çok tercih edilmiyor. Bunun yerine insanların özel günlerde birbirlerine hediye etmek için aldıkları ve belirli bir site veya uygulamaya (Netflix, Spotify…) özgü olan

sanal “gift card”lardan alıyorlar. Bunları da hacking forumlarında satarak takip edilme ihtimallerini neredeyse o’a indiriyorlar.

Saldırgan ve dolandırıcıların hedef aldıkları diğer bir sektör ise online ödeme sistemleridir (Paypal gibi). Online ödeme sistemleri, kullanıcıların dünyanın her tarafındaki e-ticaret, oyun.. sitelerinde her seferinde kart numarası girmek zorunda kalmadan kolay bir şekilde alışveriş yapmalarını sağlayan bir sistemlerdir. Bu ve bunun gibi sitelerde kullanıcıların hesaplarını ele geçirip içindeki sanal kart ve bakiyeler ile ya kendi banka hesaplarına ya da kripto para cüzdanlarına para gönderiyorlar. Dahası hiç bunlarla uğraşmayıp üst paragrafta belirtildiği gibi “gift card” satın alarak da paralarını aklayabiliyorlar.

Son olarak saldırgan ve dolandırıcılar oyun servislerine saldırıyorlar. Günümüzde online oyunlar oldukça popüler. Bu popülerlik oyun servislerine içerik satma imkanı da veriyor. Kullanıcılar oyun servislerinde ücretli içerik satın almak için kart bilgilerini giriyorlar. Bazı oyun servisleri bu bilgileri veri tabanlarında güvenliksiz bir şekilde tutuyor. Saldırganlar da bunu bildikleri için bu oyun servislerinin sunucularına saldırı düzenliyor. Ayrıca sadece kart bilgisi de değil, kişilerin başka özel bilgilerini de elde edebiliyorlar. Elde ettikleri bu bilgiler ile kişilerin mail adreslerine spam veya phishing maili gönderebilir, onları rahatsız edebilir veya bu bilgileri başkalarına satabilirler.

Sonuç

Sonuç olarak CTI (Cyber Threat Intelligence), yukarıda bahsedilen problemler için gerçek bir çözüm sunar. Saldırganların kılığına girerek onlardan alınan bilgi ile güvenliği geliştirmek ve saldırıları önlemek dünyadaki aktif siber güvenliği sağlıklı tutmaya ve zarar görmeden işlemeye devam etmesine olanak tanır.