

CYBER THREAT INTELLIGENCE

içindekiler

01

Temel Kavramlar
Siber Tehdit İstihbaratına Giriş

02

Siber Tehditler

03

CTI Nasıl Üretilir,
Analistin Rolü Nedir?

04

Zararlı Yazılımlar ve
CTI Analizi

05

APT Grupları

06

Örnek Olay
İncelemesi

Temel Kavramlar

Siber Tehdit İstihbaratına Giriş

Siber Tehdit İstihbaratının Tanımı

Siber Tehdit İstihbaratı (CTI), siber saldırılara karşı hazırlık, önlem veya müdahale eylemleri gerçekleştirebilmek amacıyla olgun kararlar verme yeteneği sağlayan; tehditler ve tehdit aktörleri hakkında aksiyon alınabilir bulgular toplanmasına ve analiz edilmesine imkan veren bilgilerdir.

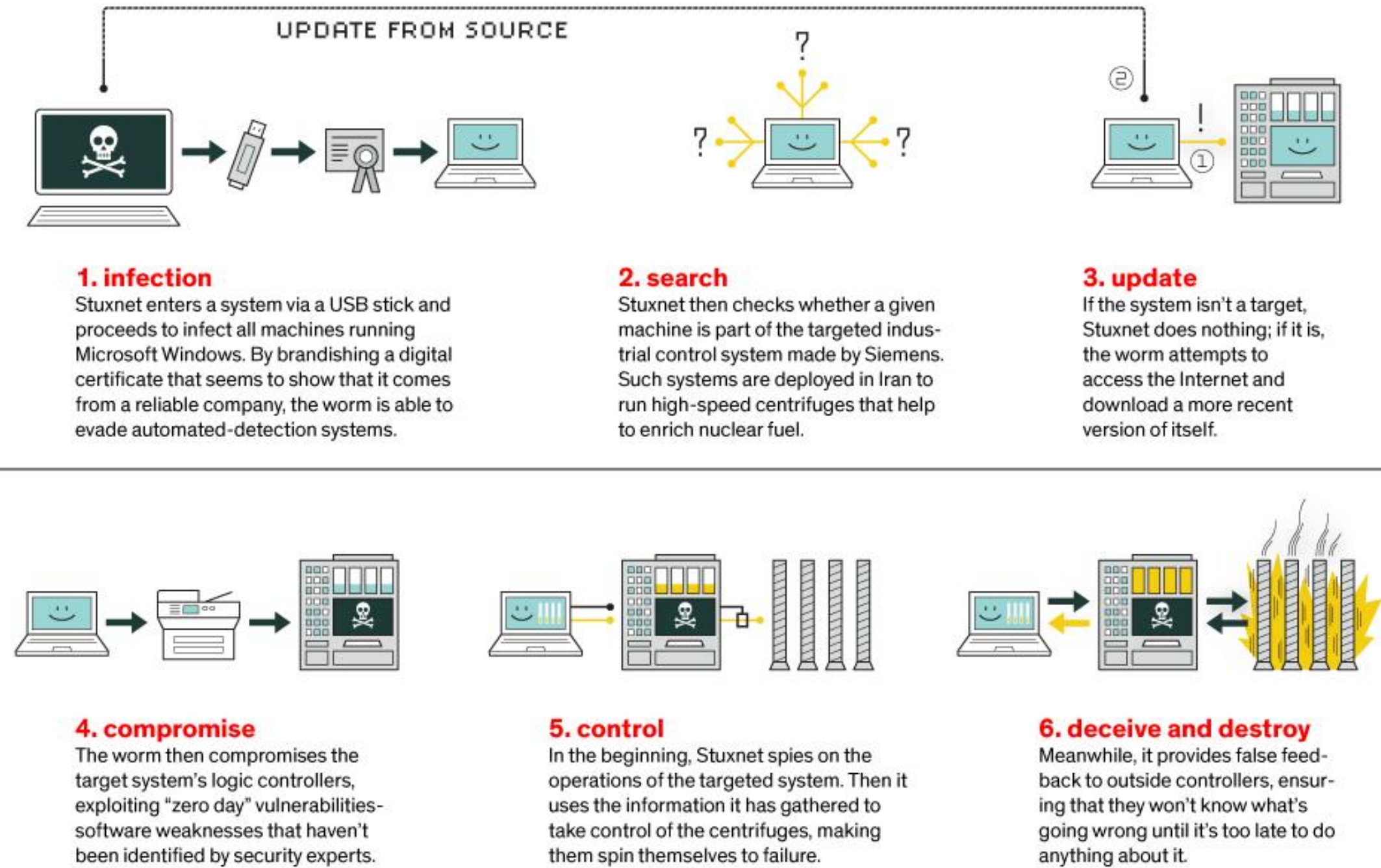
İstihbarat hem bir sonuç, hem de bu sonuca ulaşılan süreçtir.

Temel Kavramlar

Siber Tehdit: Siber Tehdit, bir kontrol sistemi cihazına ve/veya şebekesine yetkisiz erişime teşebbüs etme ya da bir bilgisayar ağını bozma olarak tanımlanmaktadır.

- Ransomware
- Phishing/Sosyal Mühendislik
- 0-day Zafiyetler
- Veri Hırsızlığı
- Siber Dolandırıcılık ve Siber Casusluk
- Hizmet Dışı Bırakma (DDoS)
- Donanım ve Teçhizata Hasar Vermek
- Kritik Altyapı Saldırıları
- Web Atakları

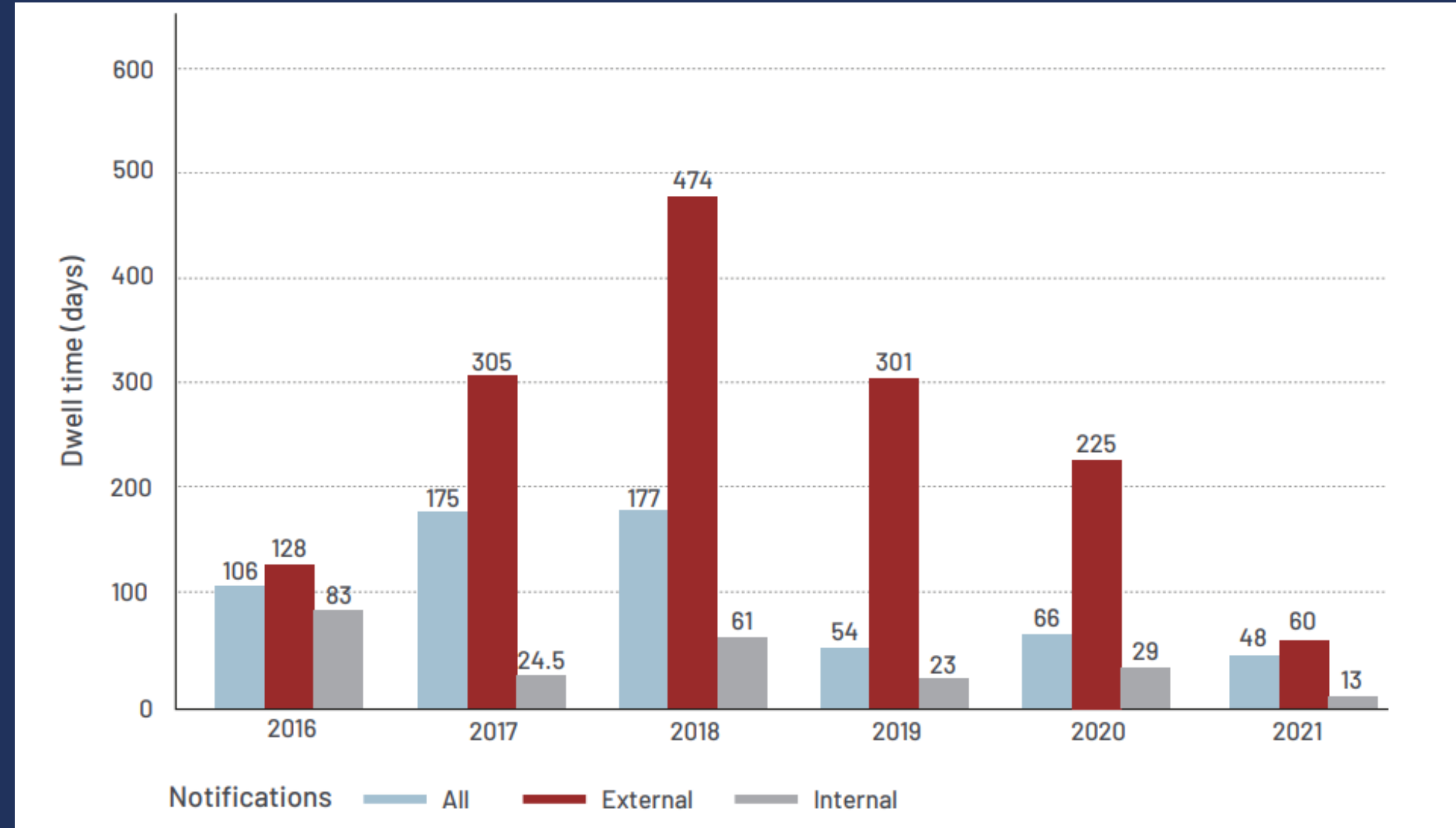
HOW STUXNET WORKED



Temel Kavramlar

Tehdit Aktörü: Kurum ve kuruluşlara yönelik tehditler, düşman hükümetler, hacktivist gruplar, terörist gruplar, hoşnutsuz çalışanlar ve kötü niyetli kişiler de dahil olmak üzere çok sayıda kaynaktan gelebilir.

Siber tehditlerle karşılaşmadan önce hazırlıklı olabilir miyiz ?



Devlet Destekli

Tehdit Aktörleri:

Bu tehdit grupları bağlı oldukları devlet tarafından çok iyi finanse edilmektedir ve sıklıkla karmaşık hedefli saldırılar gerçekleştirilmektedir. Genelde politik, ekonomik, teknik ve askeri sebeplerden kaynaklı motivasyonları/hedefleri vardır. Esas amaçları ülke çıkarlarıdır.

Organize Suç Ekipleri

Bu saldırı grupları en fazla karı getirecek eylemleri gerçekleştirmeyi tercih ederler. Genelde müşterilerin ve çalışanların sosyal güvenlik numaraları, sağlık kayıtları, kredi kartları ve bankacılık bilgileri gibi kişisel bilgileri ele geçirip bunlar üzerinden fidye alma işlemini gerçekleştirirler.

Hackivistler:

Bu saldırganlar genelde politik amaçlar gütmektedir. Amaçları propagandayı dağıtmaya yardımcı olan yüksek profilli saldırılar oluşturmak veya karşı oldukları kuruluşlara zarar vermektir. Temel amaç kendilerine fayda sağlamak ve problem olarak gördükleri bir konuya dikkat çekmektir.

Siber Teröristler:

İnternet'i, tehdit ya da yıldırma yolunu kullanarak siyasi ve ideolojik kazanımlar elde etmek amacıyla kullanmaktadırlar. Bilgisayar virüsleri, gibi araçlar aracılığıyla internete bağlı kişisel bilgisayarların ağlarını bozması gibi eylemleri içeren bir internet terör eylemi olarak kabul edilmektedir.

Casuslar:

Siber casuslar, kişilerden, rakiplerden, gruplardan, hükümetlerden; kişisel, ekonomik, politik ve askeri açıdan avantajları düşmana karşı kullanmak için bilgi edinmeye çalışırlar.

Ticari Rakipler:

Aynı endüstri içerisinde bulunan firmalar, aralarındaki ticari rekabetten dolayı karşı tarafa zarar verme girişiminde bulunabilirler. Bunu başka kurum ve kişilerle gerçekleştirebilecekleri gibi bireysel olarak da hareket edebilmektedirler.

İşinden Memnun Olmayan Mutsuz Çalışanlar

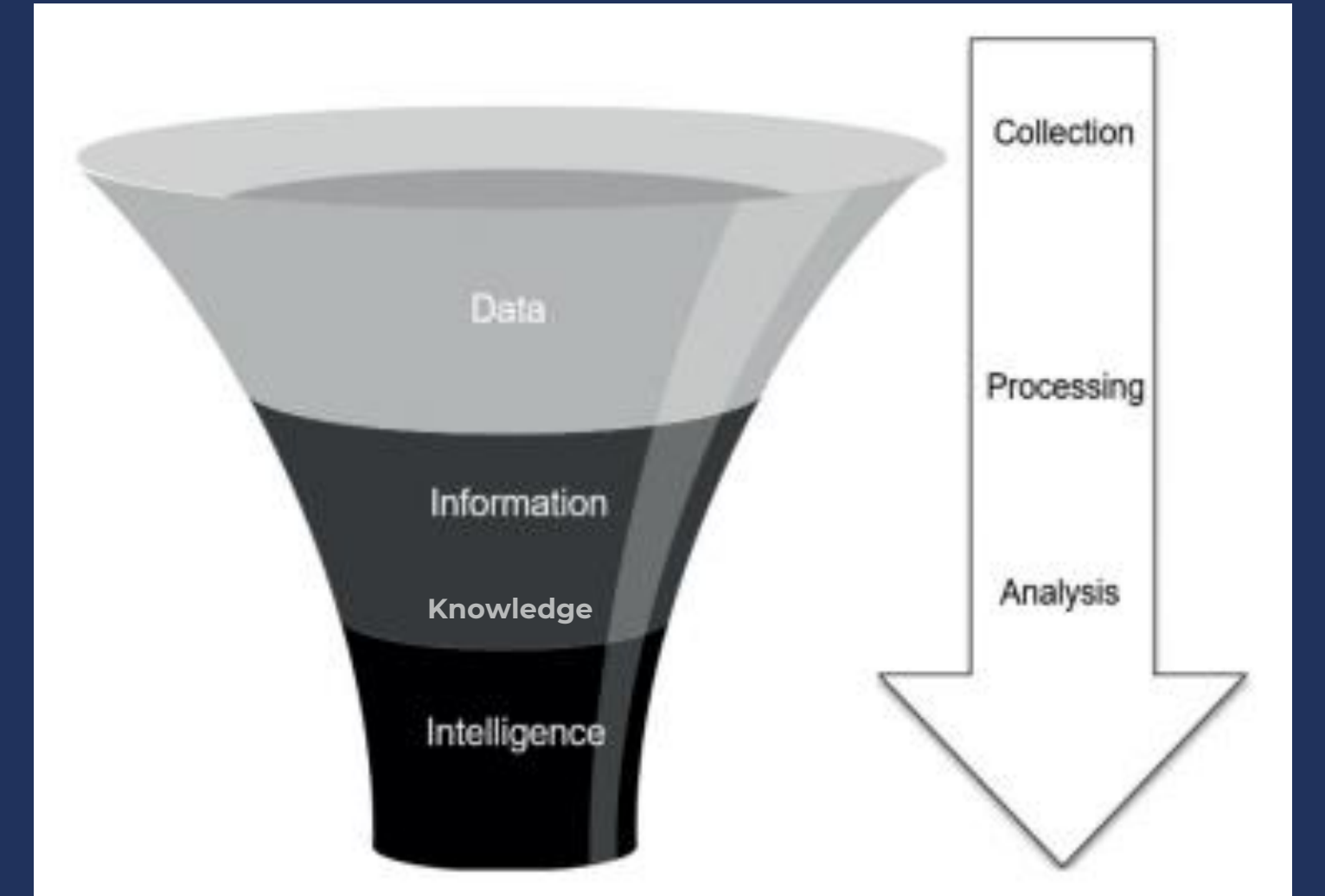
Kurumlara karşı kötü niyetli faaliyet gösteren kişilerin tamamı dışarıdan gelmek zorunda değildir. İşinden memnun olmayan, mutsuz çalışanlar daha fazla maddi kazanç elde etmek veya iş hayatında karşılaşılan tatsız olaylardan dolayı intikam almak için karşı firmalarla işbirliği yapabilirler.

Veri (Data): Bir konu hakkında araştırma, tartışma, bilgi edinme, akıl yürütme sonucunda oluşmuş olan işlenmemiş, yorum yapmaya yapmaya imkan verecek düzeyde sistemleştirilmemiş ham bilgidir.

Enformasyon (Information): Enformasyon (malumat) en genel anlamda belirli ve dar kapsamlı bir konuya ilişkin, derlenmiş bilgi parçasıdır. (Sınıflandırma)

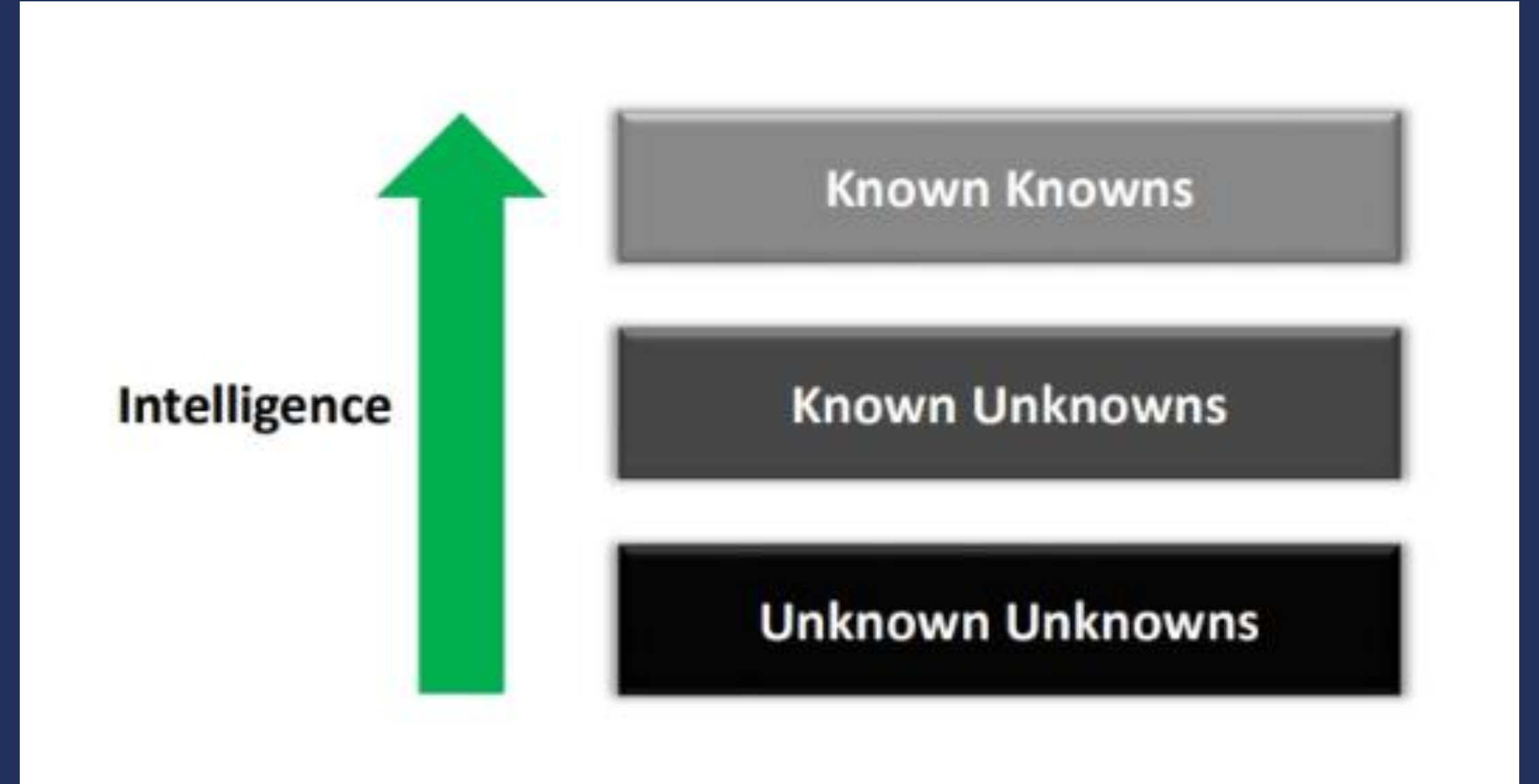
Bilgi (Knowledge): En kısa tanımıyla bilgi, işlenmiş “veri”dir. Veri, olguların harf, sayı, renk gibi sembollerle ifade edilmesi iken, bilgi, herhangi bir konu ile ilgili verilerin bir araya gelmesi ile oluşan açıklayıcı ifadeler bütünüdür. Yani verilerin akıl süzgecinden geçirilmeden önceki eliminasyonudur.

İstihbarat Hunisi



Siber Tehdit İstihbaratının Aşamaları

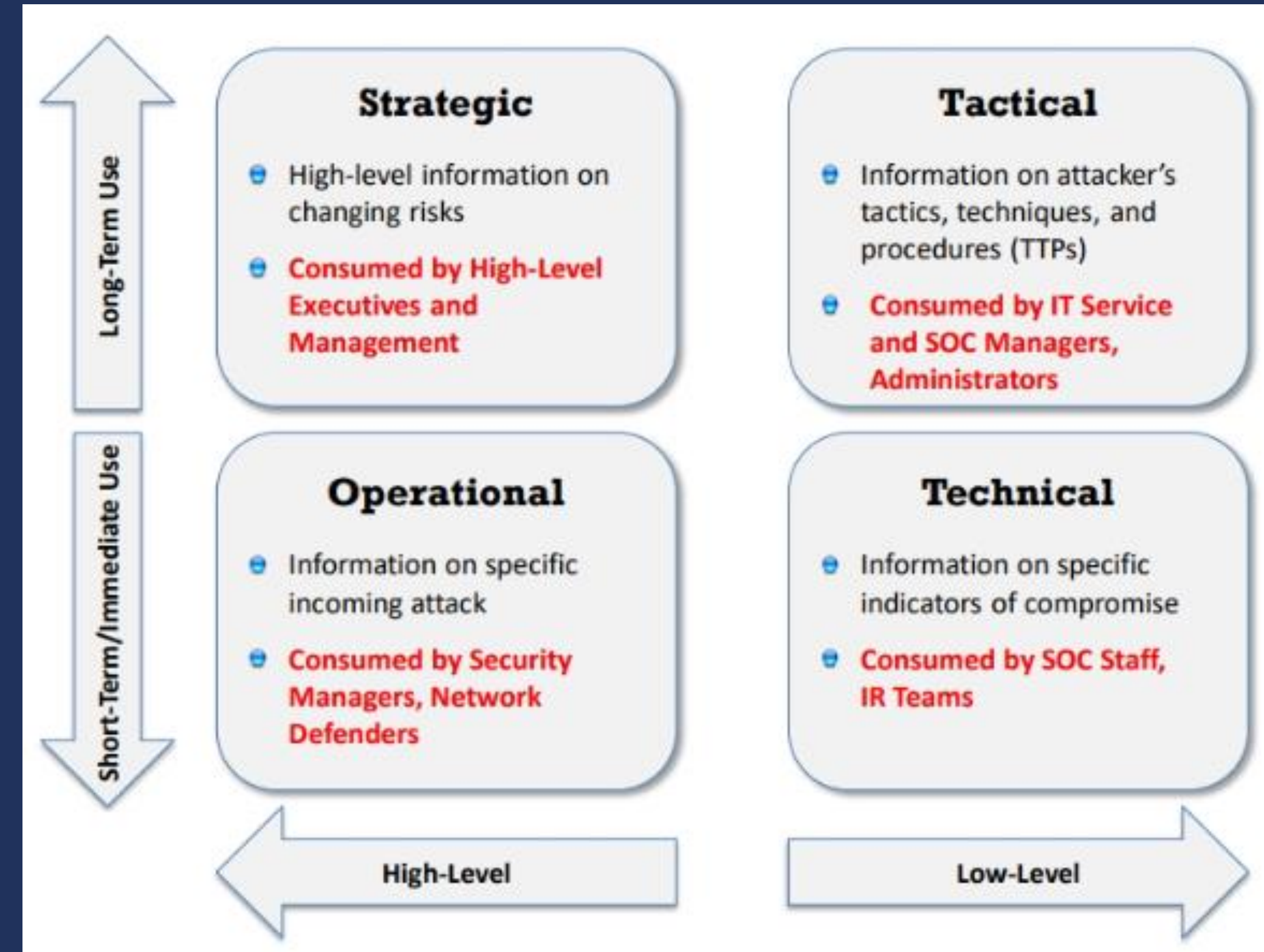
- İstihbarat süreci, tehditler hakkında hiçbir fikrimizin olmadığı ve onları bulmaya çalıştığımız “bilinmeyen bilinmeyenler” aşamasında başlar.
- Tehditlerle ilgili verileri edindikten sonra “bilinen bilinmeyenler” adı verilen ikinci aşama; tehditlerin anlamlandırılmasıyla devam eder.
- Saldırıların arkasındaki nedenler, izlenebilecek yaklaşımlar için tehdit aktörleri hakkında bilgi toplama süreci ve organizasyonların BT altyapısını koruyabilmek için alınabilecek aksiyonlar son aşamada; “bilinen bilinenler” olarak tanımlanır.



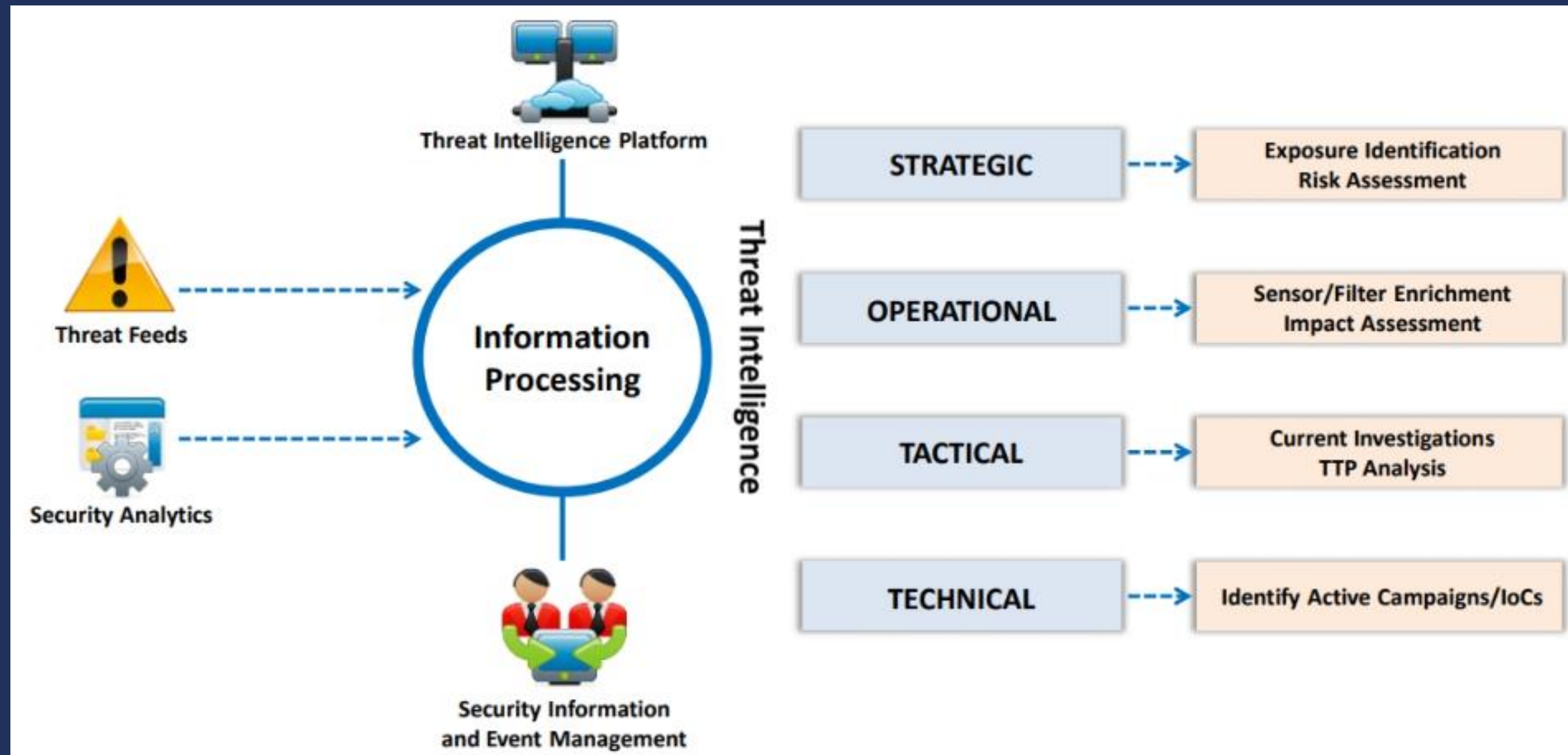
Siber Tehdit İstihbaratının Türleri

Tehdit istihbaratının türleri:

- Stratejik
- Taktiksel
- Operasyonel
- Teknik



Siber Tehdit İstihbaratının Oluşumu



İndikatör Kavramı

Indicators of Compromise (IoC)

IoC göstergeleri, bir sistem ve ağdaki olası izinsiz girişimlerin adli delilleridir. Bu deliller bilgi güvenliği uzmanları ve sistem yöneticilerinin ağa izinsiz giriş denemeleri ve diğer kötü niyetli etkinlikleri tespit etmelerini sağlar. Güvenlik araştırmacıları, belirli bir kötü amaçlı yazılımın tekniklerini ve davranışlarını daha iyi analiz etmek için IoC verilerini kullanırlar.

İndikatör Kavramı

IoC Bulguları

- Olağan Dışı Ağ Trafiği
- Yüksek Yetkili Kullanıcı Hesaplarındaki Anormallikler
- Coğrafi Aykırılıklar
- Anormal Girişler
- HTML Yanıt Boyutu
- Aynı Dosya İçinde Çok Sayıda İstek
- Veri Tabanı Okuma Hacminin Artması

SOP ve IoC İlişkisi

IP Adresleri

- Hangi ağ cihazları organizasyon için daha kritik?
- Kritik ağ cihazlarının içerden veya dışardan şüpheli/zararlı IP adresleri ile iletişimini tespit edebilmek mümkün mü?

Domain Adresleri

- Güvenlik analistlerinin domain trafiğini analiz etme kapasitesi var mı?
- Güvenlik analistleri domain adreslerine ait “whois” sorgularını analiz edebiliyor mu?

SOP ve IoC İlişkisi

URL Adresleri

- Güvenlik analistleri şüpheli/zararlı URL adreslerini ve organizasyondaki hangi kullanıcıların o adresleri ziyaret ettiğini takip edebiliyor mu?

Zararlı Yazılım Hash Değerleri ve Zararlı Dosya İsimleri

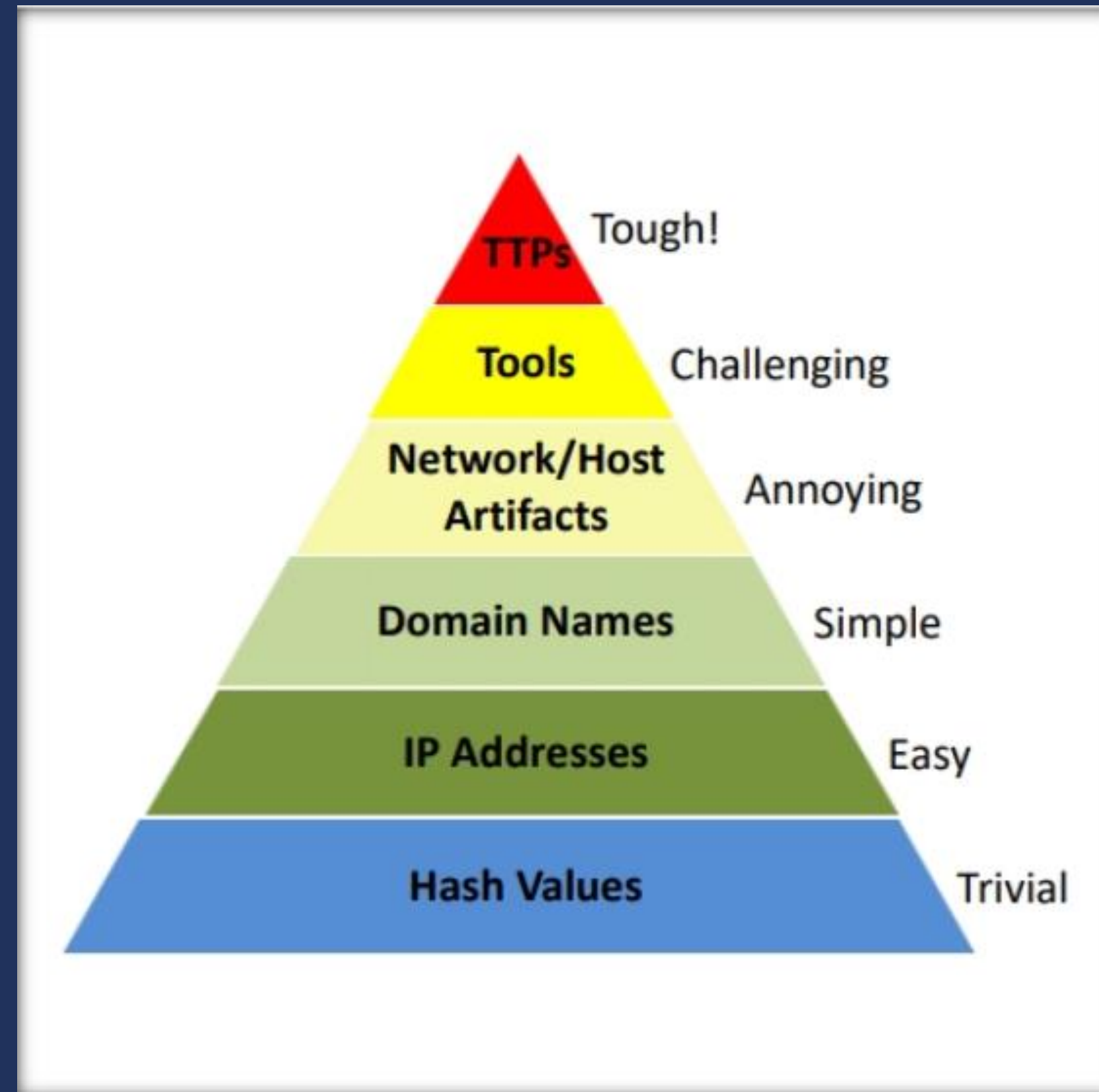
- Güvenlik analistleri organizasyondaki herhangi bir cihazda tespit edilebilecek zararlı yazılımları tespit edebiliyor mu?

Siber Tehdit İstihbaratının Güvenlik Ürünleri İle Korelasyonu

Siber güvenlik olaylarını belirleme, izleme, kaydetme, denetleme ve analiz etme gibi anlık SOC işlevlerini yerine getirmektir.

BT varlıklarının dış tehditlere karşı zarar görmesini engeller.

“Pyramid of Pain” Tanımı



Siber Tehdit İstihbaratının Önemi

- Siber tehditlere karşı derinlemesine analiz ve içgörü sağlar,
- Veri sızıntılarını ve itibar kayıplarını önler,
- Hedef alınabilecek envanterlerin yönetimini sağlar,
- Stratejik ve taktiksel kararlar alınabilmesi adına aksiyon alınabilir bulgular sunar,
- Potansiyel tehditlere karşı TTP (Teknik, Taktik ve Prosedür) sağlar.

Siber Tehdit İstihbaratı Analistlerinin Sorumlulukları

- Güncel ve doğru verilerin Deep, Surface Web, istihbarat kaynakları/araçları aracılığıyla toplanması.
- Toplanan verilerin analiz edilmesi ve siber güvenlik farkındalığına ilişkin teknik açıklamaların yapılması.
- Organizasyonun sahip olduğu risklerin belirlenmesi ve bulguların, üst düzey şirket yöneticilerine paylaşacak şekilde istihbarata dönüştürülmesi.
- Hem iç hem de dış tehdit aktörleri tarafından gerçekleştirilen saldırıların belirlenmesi, izlenmesi, değerlendirilmesi ve bunlara karşı sıkılaştırma uygulanması.
- Güncel saldırılara ait TTP bulgularının keşfedilmesi ve anlamlandırılması.

Siber Tehdit İstihbaratı Analistlerinin Sorumlulukları

- İlişkisel bilgilerin, IoC'lerin ve TTP'lerin analiz edilerek gelişen potansiyel tehditler hakkında aksiyon alınabilir istihbarat üretilmesi.
- Tehdit aktörlerinin özelliklerini ve alışkanlıklarını analiz ederek düşünce yapılarının anlaşılması.
- Etkili savunma ve sıkılaştırma stratejileri oluşturmada organizasyonlara rehberlik edilmesi.
- Zamanlamaya uygun olan tehdit raporları oluşturarak BT, olay müdahale ve SOC ekipleriyle işbirliği yapılması.

Siber Tehdit İstihbaratının Yaşam Döngüsü:

İstihbarat bulgularının toplanması, karşılaştırılması, değerlendirilmesi, ve yorumlanması sürecidir.



Siber Tehditler

Siber Saldırılar ve Atak Vektörleri

- Yetkisiz erişim elde etmek!
- Sisteme sızmak ve veri ele geçirmek

Siber Saldırı = Motivasyon + Metot + Zafiyet

Atak Vektörleri

- Cloud Tehditler
- APT Grupları
- Zararlı Yazılımlar
- Botnet Saldırıları
- Insider Tehditleri
- Phishing Saldırıları
- Web/Mobil Uygulama Tehditleri
- IoT Tehditleri

Siber Tehditler ve Kategorileri

Network Threats	Host Threats	Application Threats
<ul style="list-style-type: none">Information gatheringSniffing and eavesdroppingSpoofingSession hijacking and Man-in-the-Middle attackDNS and ARP PoisoningPassword-based attacksDenial-of-Service attacksCompromised-key attacksFirewall and IDS attacks	<ul style="list-style-type: none">Malware attacksFootprintingProfilingPassword attacksDenial-of-Service attacksArbitrary code executionUnauthorized accessPrivilege escalationBackdoor attacksPhysical security threats	<ul style="list-style-type: none">Improper data/Input validationAuthentication and authorization attacksSecurity misconfigurationInformation disclosureHidden-field tamperingBroken session managementBuffer overflow issuesCryptography attacksSQL injectionPhishingImproper error handling and exception management

Siber Tehditlerin Motivasyonu

Siber saldırıların arkasındaki genel nedenler;

- İşletme sürekliliğine zarar vermek veya bozmak,
- Bilgi hırsızlığı,
- Veri manipülasyonu,
- Kritik altyapıları bozarak korku ve kaos yaratmak,
- Hedef sektör veya firmaya finansal kayıp uğratmak,
- Dini veya siyasi inançları yaymak,
- Devletlerin askeri hedeflerini ifşa etmek, ele geçirmek, casusluk yapmak,
- İntikam almak,
- Fidyeye talep etmek.

CTI Nasıl Üretilir, Analistin Rolü Nedir?

CTI Nasıl Üretilir Analistin Rolü Nedir

- Arama motorlari (Google, Yandex, Bing)
- IoT Scanner (Shodan, Fofa, Zoomeye, Censys, Netlas.io)
- Sosyal medya
- Telegram, Discord, ICQ ve Whatsapp grupları, IRC
- Surface & Deep Web Forumları
- Ransomware Grupları

BANKA HESAPLARI SET VEYA YÜZDE OLARAK KIRAYA VERİLİR(Güvenli İşlem)

Arkadaşlar herkese merhabalar.
Tüm **banka** hesaplarımız mevcuttur.
İsteyene SET olarak, isteyene KOMİSYON karşılığında kiraya verilir.
Escrow vs. kendinizi garantiye almak isteyeceğiniz her türlü işlem kabul edilir.
Hesap sahipleri bizdedir.
Hesaplar sıfırdır, herhangi bloke durumu söz konusu değildir.


Tüm Banka Hesapları Sağlanır

Tüm Bankalara ait **hesap** kartı mevcuttur.
1K'a kadar %25, 1K üzeri işlemlerinizi için %20 pay talep edilir.
Bank Login, Kapora gibi bir sınıflandırmam yok tüm işlemleri hesaplara alabilirsiniz.

1 ADET **HESAP KARTI** + SIM CARD + İNTERNET BANKACILIĞI + **HESAP SAHİBİNE AİT ÖNLÜ ARKALI KİMLİK 3000TL**.

Yüksek tutarda ki işlemler için forum yönetimine ait Escrow **ZORUNLUDUR**.

This image has been resized. Click this bar to view the full image. The original image is sized 800x533.



CTI Nasıl Üretilir Analistin Rolü Nedir

25 Фев 2017

Доступ выдается к панели для слива, панель максимальной версии, сливает 24/7 с р...
скачивать уже слитое и уходить отжима...
150\$
Контакты под авой.
+795222004**

Продано будет 3 доступа. Первому купившему

Lalartu's second account posting his censored phone

Внимание, доступ только к email:pass/ep...

Eng_Fog
Заблокирован
Регистрация 7 Ноя 2016
Сообщения 305
Реакции 400
Баллы 130
Skype

4 Фев 2017

В наличии много доступов к почтам админ
клиентам, партнёрам, а так же по возможн
Цена за 1 почту по выборке - 1\$, цена фикс
Также можно покупать оптом по 10-50-100
Принимаю как qiwi - **7952***69*4** так и btc.
Я не несу ответственности за то что находи
Списки доступов к почте постоянно пополн

Контакты под авой.

Первым трём любая почта из списка - бесп

Xristianin, Laran112, Чихуа-Хуа и ещё 1 человек

*another part of the censored phone

CTI Nasıl Üretilir Analistin Rolü Nedir

Jmia Store										
cPannels RDPs Shells SMTPs Leads Tickets 0.00\$ My Account										
Spain	CA-Catalonia	10	1000	USER	in	Vodafone Spain	seller300	8	04/19/22 07:07:31 AM	Buy
United States	TX-Texas	2016	8G/R	ADMIN	mo**	Microsoft Azure Cloud (southcentralus)	seller491	15	04/20/22 09:08:15 AM	Buy
Spain	CT-Catalonia	10	12	USER	CL**	RIMA (Red IP Multi Acceso)	seller419	23	04/16/22 01:55:38 AM	Buy
Turkey	59-Tekirdağ	7	4	ADMIN	as**	Turk Telekomunikasyon A.S	seller434	14	04/06/22 08:34:33 PM	Buy
Canada	ON-Ontario	2019	1 GB	ADMIN	Ad**	AWS EC2 (ca-central-1)	seller434	3	04/18/22 11:47:20 AM	Buy
United Arab Emirates	DU-Dubai	2019	4	ADMIN	Co**	Microsoft Azure Cloud (uaenorth)	seller350	6	04/21/22 12:06:28 PM	Buy
United States	FL-Florida	2019	4GB	ADMIN	Ad**	Vultr Holdings, LLC	seller426	9	04/14/22 12:51:38 PM	Buy
Japan	13-Tokyo	2012	2GB	ADMIN	Ad**	AWS EC2 (ap-northeast-1)	seller481	5	04/21/22 07:49:57 AM	Buy
United States	OH-Ohio	2012	4G +	ADMIN	Ad**	AWS EC2 (us-east-2)	seller497	8	04/21/22 01:08:57 PM	Buy

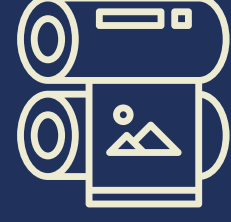
CTI Nasıl Üretilir Analistin Rolü Nedir

■		540668	10/2023	Credit Cards	Turkey	Uskudar	Uskudar	TURKIVE IS BANKASI A.S.	Buy&Check (6.5\$)
■		528208	11/2023	Credit Cards	Turkey	Antalya	Antalya	T.C. ZIRAAT BANKASI A.S.	Buy&Check (6.5\$)
■		528208	01/2023	Credit Cards	Turkey	Hatay	Hatay	T.C. ZIRAAT BANKASI A.S.	Buy&Check (6.5\$)
■		520988	09/2022	Credit Cards	Turkey	Ayd?n	Ayd?n	TURKIVE GARANTI BANKASIA.S.	Buy&Check (6.5\$)
■		493841	09/2024	Credit Cards	Turkey	Ankara	Ankara	TURKIVE VAKIFLAR BANKASIT. A. O.	Buy&Check (6.5\$)
■		482490	01/2024	Credit Cards	Turkey	Istanbul	Istanbul	TURKIVE GARANTI BANKASIA. S.	Buy&Check (6.5\$)
■		474151	09/2022	Credit Cards	Turkey	Istanbul	Istanbul	TURKIVE GARANTI BANKASIA. S.	Buy&Check (6.5\$)
■		493841	12/2022	Credit Cards	Turkey	Istanbul	Istanbul	TURKIVE VAKIFLAR BANKASIT. A. O.	Buy&Check (6.5\$)
■		517041	11/2023	Credit Cards	Turkey	Istanbul	Istanbul	TURKIVE GARANTI BANKASIA.S.	Buy&Check (6.5\$)
■		523529	09/2022	Credit Cards	Turkey	Denizli	Denizli	T.C. ZIRAAT BANKASI A.S.	Buy&Check (6.5\$)
■		518896	07/2022	Credit Cards	Turkey	Fatih	Fatih	KUVEYT TURK KATILIM BANKASI A.S.	Buy&Check (6.5\$)
■		526911	12/2023	Credit Cards	Turkey	Fatih	Fatih	FINANSBANK A.S. - ENPARA	Buy&Check (6.5\$)
■		531389	04/2024	Credit Cards	Turkey	alstanbul	alstanbul	PAPARA ELEKTRONIK PARA VE ODEME	Buy&Check (6.5\$)
■		493841	05/2024	Credit Cards	Turkey	Izmit	Izmit	TURKIVE VAKIFLAR BANKASIT. A. O.	Buy&Check (6.5\$)
■		557829	07/2023	Credit Cards	Turkey	Istanbul	Istanbul	AKBANK T.A.S.	Buy&Check (6.5\$)

CTI Nasıl Üretilir Analistin Rolü Nedir

Open Source Intelligence (OSINT)

Zararlı Yazılımlar ile Örnek Olay İncelemesi



Virüs

Bilgisayar virüsü, kullanıcının izni ya da bilgisi dahilinde olmadan bilgisayarın çalışma şeklini değiştiren ve kendini diğer dosyaların içerisinde gizlemeye çalışan bir tür bilgisayar programıdır.



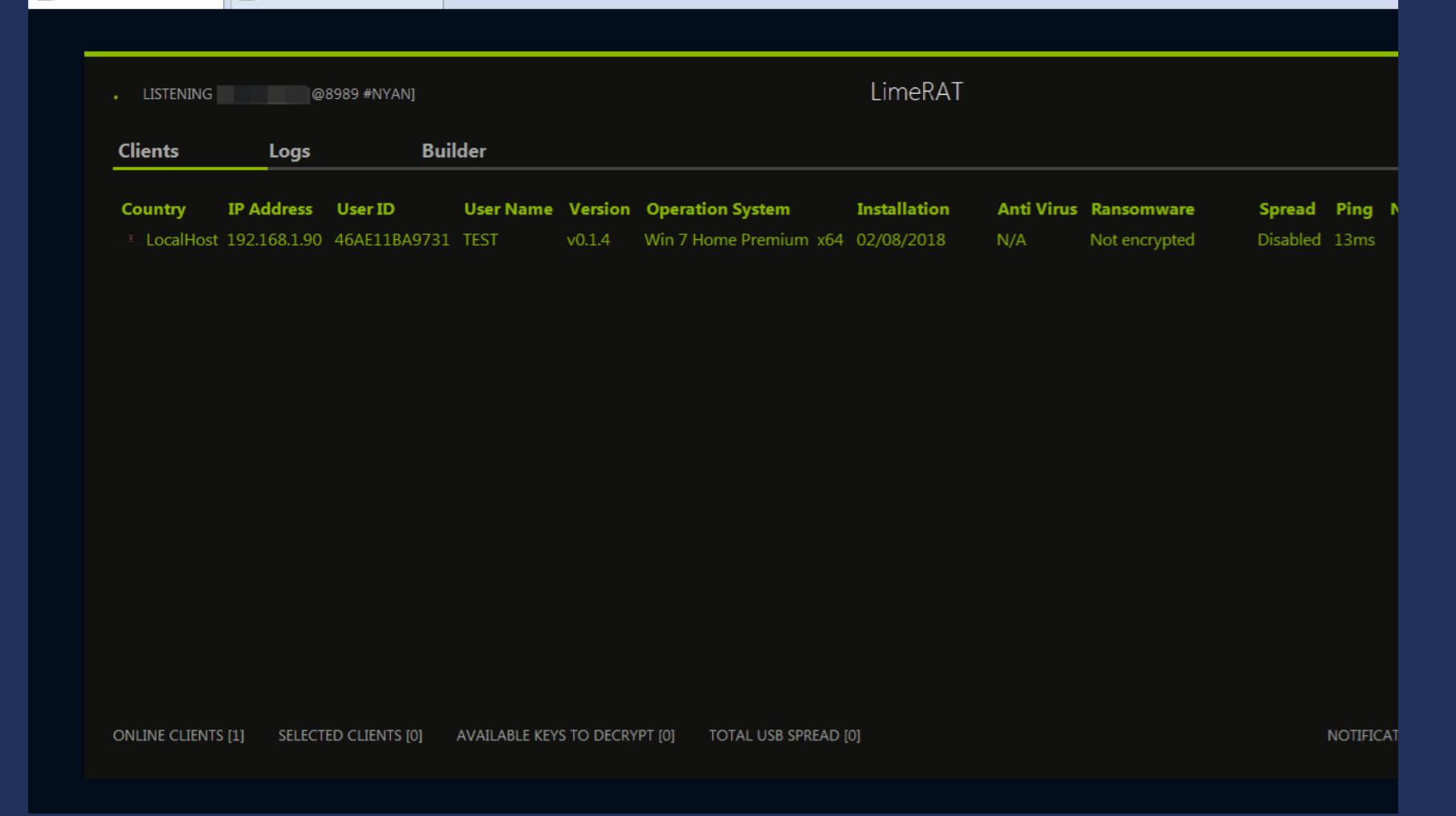
Keylogger (Tuş Kaydedici)

Kuruldukları sistemin klavye girdilerini, anlık ekran görüntülerini, sistem loglarını, program açılış ve kapanış saatlerini bilgisayar üzerinden alarak kötü niyetli kişiye gönderen programlardır.



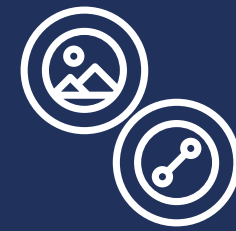
Trojan (Truva Atı)

Kurbanın içerisinde ne olduğunu bilmeden çalıştığı ve gayet masum görünen, çoğu zaman AV tarafından tespit edilemeyen yazılımlardır. Kurbanı kendi isteği ile indirilip çalıştırılır.



Worm (Solucan)

Solucanlar, virüslerin bir alt dalıdır. Kendilerini sürekli farklı cihazlara kopyalarlar. Bir bilgisayara girdiğinde diğerlerine sıçramak için cihaza takılan Flash Disk, SD Card ve CD'lere kendisini kopyalar.



Adware (Reklam Yazılımı)

Bilgisayara herhangi bir zarar vermezler ve bilgi çalmazlar. Bu yazılımları yazan saldırganlar, reklamlara tıkladıkça para kazandıkları için maddi amaçlarla bu işi yapmaktadırlar.



Ransomware (Fidye Yazılımı) Stealer Zararlı Yazılımı

Ransomware, zararlı yazılımın kurbanın bilgisayarında yaptığı değişikliklerin geri alınması için bir ödeme talebinde bulunur. Kurbanın sistemine normal olarak erişimi engellemektedir.



Stealer bulaştığı sistemlerden bilgi toplayan bir Truva zararlısıdır. Toplanan veriler tarayıcılarda kayıtlı olan kullanıcı adı, parola, kredi kartı verileri gibi özlük bilgilerini içermektedir.

443___TR[D3F0B9ABAF8B725781C2FEF0F10F5549] [2021-12-20T03_16_08.98 >

Ad	Değiştirme tarihi	Tür	Boyut
Autofills	20.12.2021 17:20	Dosya klasörü	
Cookies	20.12.2021 17:20	Dosya klasörü	
CreditCards	20.12.2021 17:20	Dosya klasörü	
Discord	20.12.2021 17:20	Dosya klasörü	
Steam	20.12.2021 17:20	Dosya klasörü	
DomainDetects.txt	20.12.2021 03:16	Metin Belgesi	1 KB
ImportantAutofills.txt	20.12.2021 03:16	Metin Belgesi	2 KB
InstalledBrowsers.txt	20.12.2021 03:16	Metin Belgesi	1 KB
InstalledSoftware.txt	20.12.2021 03:16	Metin Belgesi	3 KB
Passwords.txt	21.04.2022 22:38	Metin Belgesi	31 KB
Screenshot.jpg	20.12.2021 03:16	JPG Dosyası	169 KB
UserInformation.txt	20.12.2021 03:16	Metin Belgesi	2 KB

chimera crack - Google'da X Chimera Tool Full Crack (Güncel Versiyon 27.48)

www.youtube.com/watch

https://s3.us-east-2...

YouTube

Ara

OTURUM AÇ

Chimera Tool Full Crack (Güncel Versiyon 27.48)

38.825 görüntüleme • 9 Şub 2021

112 BEĞENME

PAYLAŞ

KAYDET

Orhan Likos

02:30

20.12.2021

Galatasaray'ın Avrupa Ligi Grup Maçları | EXXENSPOR

EXXENSPOR

477 B görüntüleme • 6 gün önce

Yeni

TAKTİK REKABET: Pep Guardiola vs Jürgen Klopp

Hastalık Bu Futbol

354 B görüntüleme • 1 yıl önce

F1'de Yeni Dönem, Yeni Araçlar & Kurallar, 2022'de Neler...

Socrates Dergi

187 B görüntüleme • 5 ay önce

Kobe Bryant 81 Sayılık Maç Kaan Kural & Murat...

Alihan Olcar

1,8 Mn görüntüleme • 1 yıl önce

DUNE Analizi

Başış Özcan

1,2 Mn görüntüleme • 1 ay önce

Çok Güzel Hareketler 2 - 103 Bölüm

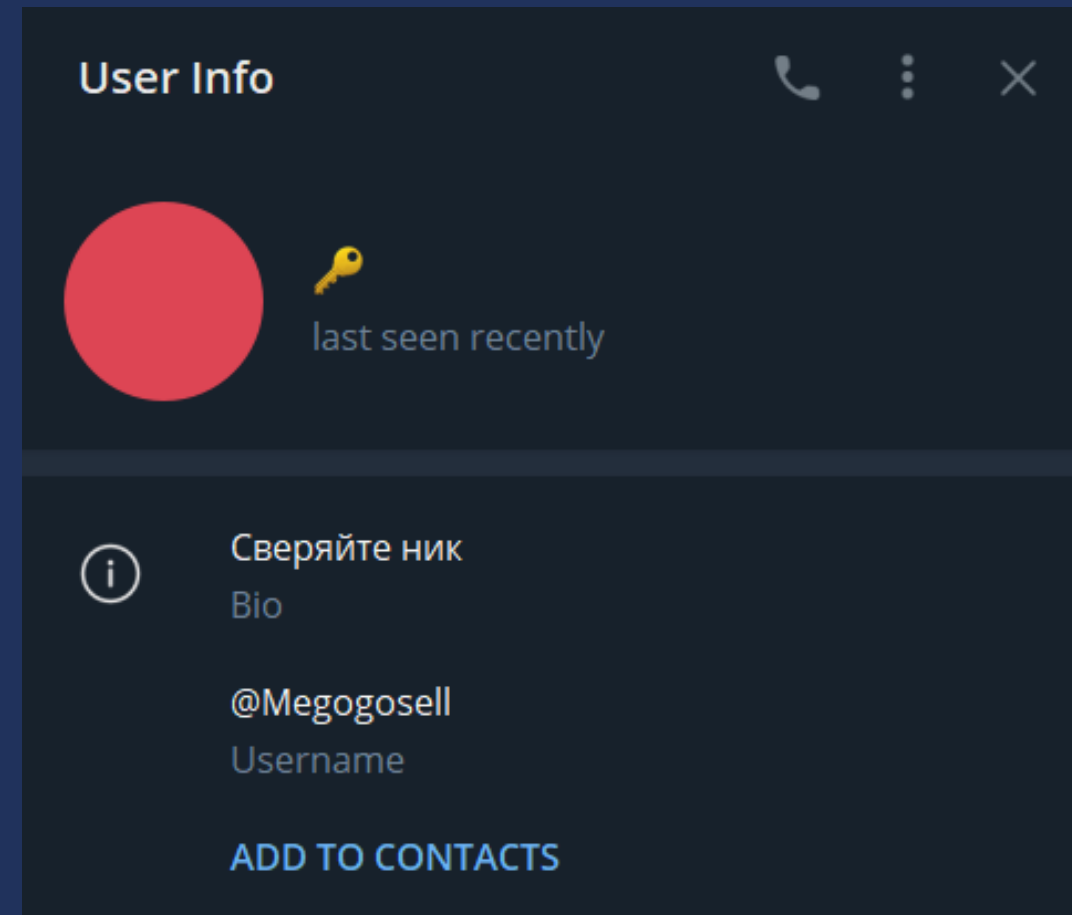
```
*****
*
*
* [REDACTED]
*
* Telegram: https://t. [REDACTED]
*
*****

Build ID: @MegogoSell Stealer Zararsini Dağtan Tehdit Aktörünün Kullanıcı Adı
IP: 88.230.2 [REDACTED] Kurbann IP Adresi
FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
UserName: nazik
Country: TR
Zip Code: 35240
Location: Izmir, Izmir
HWID: D3F0B9ABA [REDACTED]
Current Language: Turkish (Turkey)
ScreenSize: {Width=1920, Height=1080}
TimeZone: (UTC+03:00) Istanbul
Operation System: Windows 10 Home x64
UAC: AllowAll
Process Elevation: False
Log date: 12/20/2021 3:16:08 AM

Available KeyboardLayouts:
Turkish (Turkey)

Hardwares:
Name: Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz, 4 Cores
Name: NVIDIA GeForce GTX 1060 3GB, 3221225472 bytes
Name: Total of RAM, 8134.65 MB or 8529797120 bytes

Anti-Viruses:
Windows Defender
```



```
*****
*
* [REDACTED]
*
* Telegram: https://t.me/REDLINESUPPORT
*
*****

URL: https://giris.hepsiburada.com/
Username: [REDACTED]@gmail.com
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
URL: https://auth.riotgames.com/login
Username: [REDACTED]
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
URL: https://isube.payfix.com.tr/register
Username: [REDACTED]
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
URL: https://accounts.google.com/signin/v2/sl/pwd
Username: [REDACTED]
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
URL: https://discord.com/login
Username: [REDACTED]
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
URL: https://steamcommunity.com/openid/login
Username: [REDACTED]
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
```

Tehdit Verisi Beslemeleri

Zararlı URL'ler/ Botnet C&Cs

Zararlı bağlantıları ve web sitelerini kapsayan bir dizi URL içermektedir.

abuse.ch

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2022-04-22 05:54:05	http://182.124.94.251:53955/i	Online	32-bit elf mips Mozi	@geenensp
2022-04-22 05:51:06	http://61.52.90.194:50009/Mozi.m	Online	elf Mozi	@lrz_urlhaus
2022-04-22 05:51:05	http://39.72.213.216:53637/Mozi.m	Online	elf Mozi	@lrz_urlhaus
2022-04-22 05:51:05	http://59.99.137.220:52956/Mozi.m	Online	elf Mozi	@lrz_urlhaus
2022-04-22 05:51:05	http://61.53.88.38:59415/Mozi.m	Online	elf Mozi	@lrz_urlhaus
2022-04-22 05:51:05	http://222.138.117.225:52768/Mozi.m	Online	elf Mozi	@lrz_urlhaus
2022-04-22 05:51:04	http://223.130.30.6:55905/mozi.m	Offline		@tammeto
2022-04-22 05:50:06	http://163.179.170.164:52310/Mozi.a	Online	elf Mozi	@lrz_urlhaus
2022-04-22 05:48:04	http://119.179.250.120:53159/i	Online	32-bit elf mips Mozi	@geenensp
2022-04-22 05:36:10	http://222.141.45.154:44260/Mozi.m	Online	elf Mozi	@lrz_urlhaus
2022-04-22 05:36:10	http://58.53.59.98:53809/Mozi.a	Online	elf mirai Mozi	@lrz_urlhaus
2022-04-22 05:36:10	http://27.45.57.177:40466/Mozi.m	Online	elf mirai Mozi	@lrz_urlhaus
2022-04-22 05:36:10	http://60.215.36.19:51820/Mozi.a	Online	elf mirai Mozi	@lrz_urlhaus
2022-04-22 05:36:09	http://27.43.109.63:46079/Mozi.m	Online	elf mirai Mozi	@lrz_urlhaus

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2022-04-22 04:20:24	1.161.126.64	QakBot	Online	AS3462 HINET Data Communication Business Group	TW
2022-04-22 01:50:12	1.161.126.64	QakBot	Online	AS3462 HINET Data Communication Business Group	TW
2022-04-21 15:50:32	31.215.214.189	QakBot	Offline	AS5384 EMIRATES-INTERNET Emirates Internet	AE
2022-04-21 14:10:57	72.252.157.172	QakBot	Offline	AS30689 FLOW-NET	JM
2022-04-21 14:10:52	140.0.79.30	QakBot	Offline	AS23700 FASTNET-AS-ID Linknet-Fastnet ASN	ID
2022-04-21 14:10:30	189.253.162.110	QakBot	Offline	AS8151 Uninet S.A. de C.V.	MX
2022-04-21 13:45:54	201.172.23.68	QakBot	Offline	AS11888 Television Internacional, S.A. de C.V.	MX
2022-04-21 13:45:50	174.95.174.163	QakBot	Online	AS577 BACOM	CA
2022-04-21 13:45:49	31.215.214.189	QakBot	Offline	AS5384 EMIRATES-INTERNET Emirates Internet	AE
2022-04-21 13:45:46	41.84.248.41	QakBot	Offline	AS19711 SWAZINET	SZ
2022-04-21 11:15:19	85.97.79.239	QakBot	Offline	AS9121 TTNET	TR

Tehdit Verisi Beslemeleri

Oltalama URL'leri

Kimlik avı saldırılarında ve zararlı yazılım kampanyalarında kullanılan güncel URL bilgilerini içermektedir.

An Anubis Botnet Incident Turkey

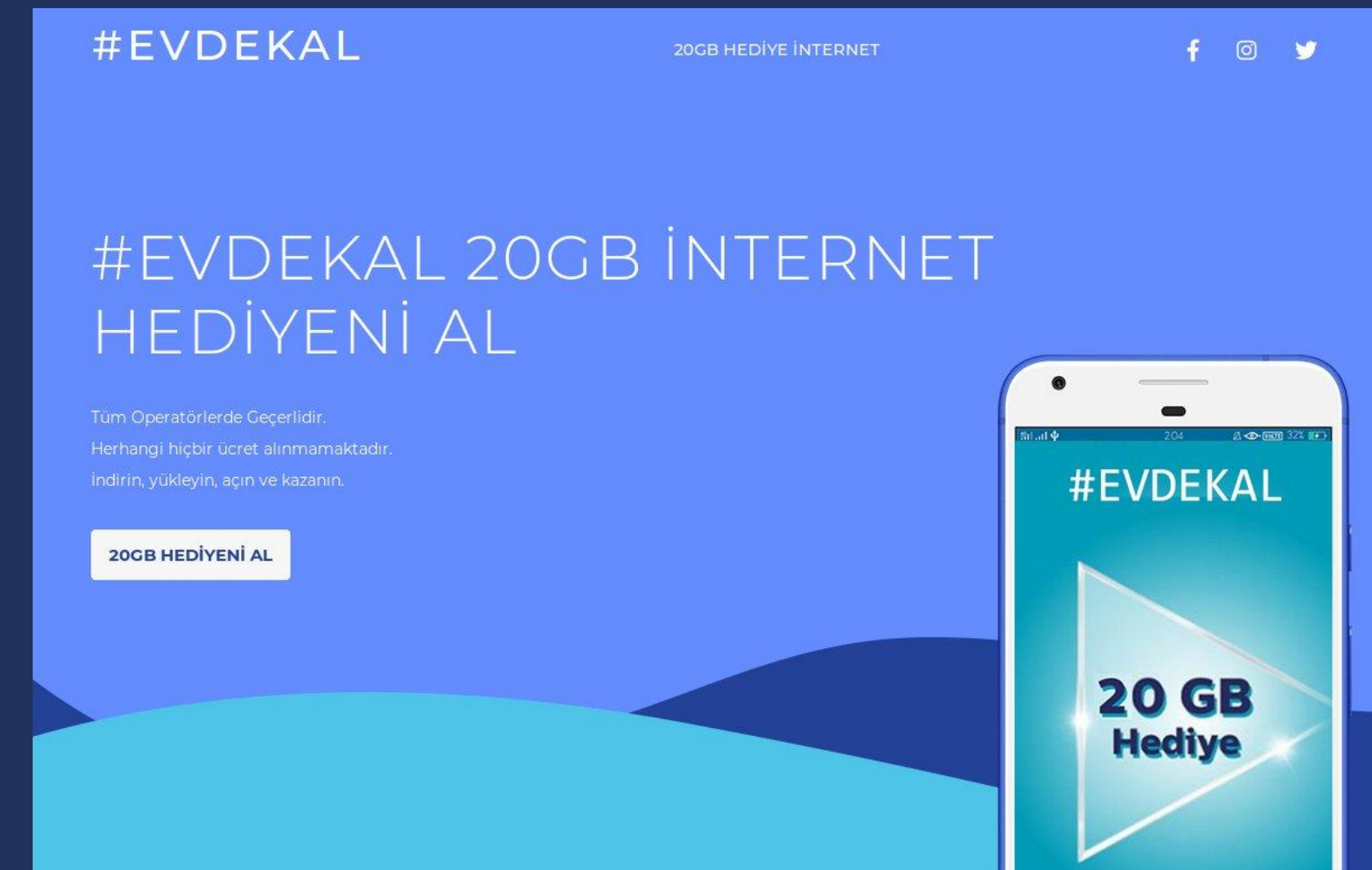
IOC

From: evdekal20gbdestektr[.]com

Name: 20gb_hediye_internet.apk

Hash:"1862cd3b830b9373d7c8f3f64e74de3c54c12f47a6c52c9c9d0bfcbe51a29e3f"

[virustotal.com/gui/file/1862c...](https://www.virustotal.com/gui/file/1862c...)



Tehdit Verisi Beslemeleri

Botnet C&C URL'leri

Zararlı yazılımların iletişim kurmuş oldukları Komuta ve Kontrol sunucularına ait URL adreslerini ve bunlara ait IP adreslerini içermektedir.

A Covid-19 Cerberus Botnet Incident

IOC

From: virus-covid[.]online

Name: covidMappia_v1.0.3.apk

Hash:"70439d393cca65ede64971d923ed61c0dd332dad5e2c31fdf8d225db1cf933e8"

[virustotal.com/gui/file/70439...](https://www.virustotal.com/gui/file/70439d393cca65ede64971d923ed61c0dd332dad5e2c31fdf8d225db1cf933e8)

Main BOTS table

Delete selected bots Filter table Select All on this page Clear selection

ID	Version	Mode	Country	Uptime	Status	Date Infection	Comment
d1xgrjykyplh0g4ho	8.1.0	TEST	Germany	1d	Dead	2019-06-21 18:47	Мёртвый бот
u1frksjxdwej8pno3	8.1.0	TEST	Germany	17h	Online	2019-06-22 15:14	
erhc8335xmqrdr42s	8.1.0	TEST	USA	12h	Online	2019-06-22 20:58	
klhv947uy2vdv327a	8.1.0	TEST	USA	12h	Online	2019-06-22 21:02	

1

Send sms
Send sms from selected bots
Phone number +1...
SMS Text
Send SMS

Send USSD
Send USSD from selected bots
*999# USSD
Send USSD

Forward call
Forward call on selected bots
Phone number +1...
Forward calls

Bots: 4 | Online: 0 | Offline: 4 | Dead: 0
Banks: 4 | Cards: 2 | Mails: 4
Cerberus Android Bot 1.5.0.9

Tehdit Verisi Beslemeleri

Zararlı Yazılım Hash'leri

Geçmişteki ve günümüzdeki zararlı yazılımlara ait dosya hash'lerini içermektedir. Böylece imza tabanlı antivirüsler ile sistemler korunabilmektedir.

Main object - "SQLi32bit.exe"		?	☑
SHA256	008EB1BDD700BC0638FC63CEA71E3A8EF8730AFD9E25C5CE24DCBDDF811D8F66	?	☑
SHA1	6E722DEEC7AF2DEEF32FD52736783FE222E5AD14	?	☑
MD5	FEC5156D1A8A0D023E835403FCE004D9	?	☑
Dropped executable file		?	☑
SHA256	C:\Users\admin\AppData\Local\Temp\Setup.exe 75F58DCB358452EA8DB7F9A749D507B09A9D98A19B772D404EC453F39D645391	?	☑
SHA256	C:\Users\admin\AppData\Local\Temp\~SQLi_v_9_8_2.exe D430BC4B72CF86DD0E0820FDC0FB87D3A389529BC8F8B8950C902F996A228A	?	☑
SHA256	C:\Users\admin\AppData\Roaming\Intel Corporation\Intel(R) Common User Interface\8.1.1.7800\svchos t.exe E369BEB5EFAFD39DA1705D70892329EDF863324B73EA22175C8A7B0150296BAB	?	☑
SHA256	C:\Users\admin\AppData\Roaming\Microsoft\Windows\8.1.7601.17587\svchost.exe D65481B5047A251D9F3115AD4CF10A3013BE63623847A322C3FBD8B71242E39D	?	☑

FileHash-SHA1	c63f79a828505270f0ddf90117a1ca5f0c231801	Trojan.Spy.Stealer.MSIL.Generic	Apr 27, 2020, 11:57:03 PM
FileHash-MD5	96bd7735f1e2f6e9071ffb8c87a798fe	Trojan.Spy.Stealer.MSIL.Generic	Apr 27, 2020, 11:57:03 PM
FileHash-SHA1	8d3b4ded7ed09acdaef7e68d70a007419bda4abc	Win32.Downer.PUA	Apr 27, 2020, 11:57:03 PM
FileHash-MD5	28897de097b5a78a55fe5166c7bdc414	Win32.Downer.PUA	Apr 27, 2020, 11:57:03 PM
hostname	pc6.down2.99downer.com	Win32.Downer.PUA	Apr 27, 2020, 11:57:03 PM
FileHash-SHA1	cfdc2628f829fa149e41fd043d731f20a6491aa3	Trojan.Win32.A.Vigorf	Apr 27, 2020, 11:57:03 PM
FileHash-MD5	6bf15ca0278346b865110b3af0a52538	Trojan.Win32.A.Vigorf	Apr 27, 2020, 11:57:03 PM
FileHash-SHA1	505daeb829431bb61122cba3321958f0f9935deb	Backdoor.Linux.B.Mirai	Apr 27, 2020, 11:57:03 PM
FileHash-MD5	2031bd704c2a24d4987f613f2ceae706	Backdoor.Linux.B.Mirai	Apr 27, 2020, 11:57:03 PM
FileHash-SHA1	2433ed18d9ab1cc15b389eebfd1718d8511e3b07	Trojan.Win32.Omgz.Scar	Apr 27, 2020, 11:57:03 PM

Tehdit Verisi Beslemeleri

Android/IOS Zararlı Yazılım Hash'leri



Siber uzaydaki bütün teknikler ve zararlılar yalnızca sistemlerde ve sunucularda gerçekleşmemektedir. Bunlar içerisinde Android ve IOS üzerinde paylaşılan zararlılar da vardır. İnternete açık APK'lar ve işletim sistemlerine ait uygulama satın alma noktalarındaki uygulamalar sürekli olarak taranarak zararlı tespiti gerçekleştirilmelidir.



 **Juan José Ruiz** @jjruiz · Apr 27, 2020
 Replying to @jjruiz and 2 others
 #malware #3: easy13.ru.com (#Trojan #Cerberus with md5 493f2107a91f649cbc0e2409e809aa42). Proofs on #virustotal [virustotal.com/gui/file/f6f85...](https://www.virustotal.com/gui/file/f6f85...)


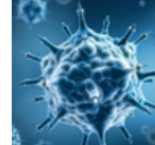
 **Juan José Ruiz** @jjruiz
 #malware #4: [http://sadclub .top/](http://sadclub.top/) (#Trojan #Cerberus with md5 76fd24ecf7bb6c25c62040ca6a059c13). Proofs on #virustotal [virustotal.com/gui/file/b571a...](https://www.virustotal.com/gui/file/b571a...)



12:59 AM - Apr 27, 2020

[See Juan José Ruiz's other Tweets](#)

  **covid-19 (info.abc.pk)** Detected
 17425e66428e284c2da73f3a7173e4291fb0b2bc76fd6d618921a9f0eb543340
 Apr 27, 2020 7:04:49 AM - Android

  **Covid-INFO (dssrege.idrnmd.chqy)** Detected
 5451a9be3d3adfed160a158a59aec0e448341e8d30ab9463c76ba08d5a48d10f
 Apr 21, 2020 9:45:23 PM - Android

  **corona virus. covid 19 news (com.my.photo.effect)** Detected
 bdf28409c52a2f527718b9ebffb8c4f0bec8384675d9d41f16914c724ded9e28
 Apr 17, 2020 6:21:06 PM - Android

  **Covid-19 Mobile (byqazjrlrfealtpf.cddlprjbsf.wmfl)** Detected
 25198fc9fdb3d4c5312702979d0d52072c359829e0bf4902c9ba171fc7538f23
 Apr 15, 2020 1:43:49 PM - Android





Aktif Ortalama Saldırıları İle Örnek Olay İncelemesi

Örnek Olay İncelemesi

Ortalama İçerikli Giriş Paneli Örneği

vakifkampanyagiris.ga/hav/index.php

ID	Sayfa	TCKN	Şifre	TELEFON	Tarih	IP	İşlem
4669	Ana Sayfa	27	274446	54	15.02.2022 11:25	78.173.52.220	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4668	Onay Ekranı	30	426538	50	15.02.2022 11:23	88.230.23.150	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4667	Onay Ekranı	40	320509	50	15.02.2022 11:11	5.47.51.93	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4666	Ana Sayfa	20	215487	Te	14.02.2022 16:25	176.54.168.131	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4665	Onay Ekranı	30	065056	53	14.02.2022 16:13	176.90.188.99	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4664	Onay Ekranı	40	340853	05	14.02.2022 16:05	46.154.73.232	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4663	Onay Ekranı	30	162160	54	14.02.2022 15:51	88.247.32.206	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4662	Onay Ekranı	40	251995	54	14.02.2022 15:39	178.244.82.6	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4661	Ana Sayfa	10	286025	53	14.02.2022 15:35	94.54.21.115	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4660	Onay Ekranı	10	240816	05	13.02.2022 22:39	88.233.235.98	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4659	Onay Ekranı	30	417114	05	13.02.2022 22:35	46.154.222.35	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4658	Ana Sayfa	30	969696	05	13.02.2022 22:30	176.232.180.115	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4657	Onay Ekranı	10	147369	05	13.02.2022 22:28	46.221.64.82	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4656	SMS Sayfası	10	306306	55	13.02.2022 22:24	176.33.116.94	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4655	Onay Ekranı	30	788171	05	13.02.2022 21:34	176.219.196.144	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4654	Onay Ekranı	50	147258	05	13.02.2022 21:33	78.190.22.67	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4653	Onay Ekranı	20	252525	05	13.02.2022 21:30	88.234.195.137	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4652	Onay Ekranı	60	533052	53	13.02.2022 21:28	5.176.241.171	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA
4651	Onay Ekranı	10	634638	50	13.02.2022 21:24	5.46.195.104	BAŞA YOLLA BAN BAN TC SIL ONAYA ZORLA

Conti Leaks ile Örnek Olay İncelemesi

Örnek Olay İncelemesi

Conti Tehdit Aktörü Veri Sızıntısı Analizi

Rusya devlet ile ilişkili olduğu düşünülen Conti Ransomware grubuna ait 60.000 dahili mesaj, sunucu giriş bilgileri, çeşitli zararlı yazılımlara ait C2 (command-and-control) sunucuları, fidye pazarlığının yapıldığı Conti Recovery servisine ait bilgileri ve Conti'nin siber saldırıları, bu saldırılarda kullandığı teknik-taktik-prosedürleri (TTPs) yer almaktadır.

> Greetings,

Here is a friendly heads-up that the Conti gang has just lost all their shit. Please know this is true.

<https://twitter.com/ContiLeaks/status/1498030708736073734>

The link will take you to download an 1.tgz file that can be unpacked running `tar -xzvf 1.tgz` command in your terminal . The contents of the first dump contain the chat communications (current, as of today and going to the past) of the Conti Ransomware gang. We promise it is very interesting.

There are more dumps coming , stay tuned.
You can help the world by writing this as your top story.

It is not malware or a joke.
This is being sent to many journalists and researchers.

Thank you for your support

Glory to Ukraine!

Örnek Olay İncelemesi

Jabber chat logları incelendiğinde, Conti Ransomware grubuna ait 30 adet Linux sunucu keşfedilmiştir.

```
"body": "root 45.86.74.108 123qweASDzxc\nroot 5.181.80.125 123qweASDzxc\nroot 185.99.132.248 P*1rM@WzYm42q8\n\nroot 5.39.63.107 123qweASDzxc\nroot 158.69.133.72 123qweASDzxc\nroot 23.254.228.234 Y8Tn7WVsPuJqbRpsFd\n\nroot 194.36.191.19 123qweASDzxc\nroot 194.40.243.33 S9m7LTV3e756\n\nroot 23.160.193.217 zclqqwouwfqk\n\nroot 176.103.62.176 Hzy59gDZ BG\n\nroot 94.140.113.71 pEJeI19zqkwnLmW LV\n\nroot 146.19.253.90 xctY2gds98oXNtwj NL\n\nroot 38.92.191.89 xSRs9Up8Vtb9xQHC US\n\n\nroot 5.2.78.37 97552266b2397be148cb626180bff4c1 NL\n\nroot 198.244.194.4 oGYMvME2d6U8wzis UK\n\nroot 80.92.206.199 zwyfmtCmBt8H NL\n\nroot 45.14.226.23 zNJ2432Uc7rk7Lod NL\n\nroot 185.38.185.13 M7s8C0x6 NL\n\n\nroot 45.41.204.137 v@hgcYCinp1B\n\n\nroot 94.140.113.17 o6tyGMzP5ufZplo\n\n\nroot 139.28.235.177 123qweASDzxc\n\n\nroot 5.181.80.143 0.00009531\n\n\nroot 185.99.132.67 s*z2O9P6H9L@bp\n\n\nroot 5.39.63.108 123qweASDzxc\n\n\nroot 192.99.255.38 123qweASDzxc\n\n\nroot 142.11.253.72 pbsfkJyKg5R5M4\n\n\nroot 185.106.123.88 123qweASDzxc\n\n\nroot 45.41.204.139 %aCBKb0mN8qF"
```

- [root 45.86.74.108 123qweASDzxc](#)
- [root 5.181.80.125 123qweASDzxc](#)
- [root 185.99.132.248 P*1rM@WzYm42q8](#)
- [root 5.39.63.107 123qweASDzxc](#)
- [root 158.69.133.72 123qweASDzxc](#)
- [root 23.254.228.234 Y8Tn7WVsPuJqbRpsFd](#)
- [root 194.36.191.19 123qweASDzxc](#)
- [root 194.40.243.33 S9m7LTV3e756](#)
- [root 23.160.193.217 zclqqwouwfqk](#)
- [root 176.103.62.176 Hzy59gDZ BG](#)
- [root 94.140.113.71 pEJeI19zqkwnLmW LV](#)
- [root 146.19.253.90 xctY2gds98oXNtwj NL](#)
- [root 38.92.191.89 xSRs9Up8Vtb9xQHC US](#)
- [root 5.2.78.37 97552266b2397be148cb626180bff4c1 NL](#)
- [root 198.244.194.4 oGYMvME2d6U8wzis UK](#)
- [root 80.92.206.199 zwyfmtCmBt8H NL](#)
- [root 45.14.226.23 zNJ2432Uc7rk7Lod NL](#)
- [root 185.38.185.13 M7s8C0x6 NL](#)
- [root 45.41.204.137 v@hgcYCinp1B](#)
- [root 94.140.113.17 o6tyGMzP5ufZplo](#)
- [root 139.28.235.177 123qweASDzxc](#)
- [root 5.181.80.143 0.00009531](#)
- [root 185.99.132.67 s*z2O9P6H9L@bp](#)
- [root 5.39.63.108 123qweASDzxc](#)
- [root 192.99.255.38 123qweASDzxc](#)
- [root 142.11.253.72 pbsfkJyKg5R5M4](#)
- [root 185.106.123.88 123qweASDzxc](#)
- [root 45.41.204.139 %aCBKb0mN8qF](#)

Örnek Olay İncelemesi

Tespit edilen sunuculara SSH bağlantısı yapmadan önce operasyon güvenliği (OPSEC) sağlanmalıdır. Operasyon güvenliği sağlandıktan sonra makine içinde keşif yapılmalıdır.

Tehdit aktörlerinin sunucu içerisinde birçok sıkılaştırma yaparak yanal hareketi kısıtladığı görülmüştür.

Örneğin, /root dizininde bulunan ".bash_history, .bashrc, .cache, .ssh/known_hosts" dosyalarının binary'leri değiştirilerek bozulduğu ve Tab tuşu ile otomatik doldurmanın devre dışı bırakıldığı tespit edilmiştir.

```
root@candan:~# firejail --seccomp --nonewprivs --private-tmp torify ssh root@91.193.181.22 -p1021
Reading profile /etc/firejail/server.profile
Reading profile /etc/firejail/disable-common.inc
Reading profile /etc/firejail/disable-passwdmgr.inc
Reading profile /etc/firejail/disable-programs.inc

** Note: you can use --noprofile to disable server.profile **

Parent pid 5446, child pid 5447
The new log directory is /proc/5447/root/var/log
Child process initialized in 34.02 ms
The authenticity of host '[91.193.181.22]:1021 ([91.193.181.22]:1021)' can't be established.
ECDSA key fingerprint is SHA256:dn6gwyJZPpkzXMRpsGgXoUpJutKpFgn7a1JaTCMBzNE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[91.193.181.22]:1021' (ECDSA) to the list of known hosts.
root@91.193.181.22's password: █
```

```
root@e20178:~# cat .bashrc
7?fv<UYOüçπg;auY&dğ#HrOeM05
MoY
Xd>Q, YQ~@0i0
#d>X iJXF>7!XAs0B=dV-ε&UH%q X2
Nw<W>)n&l|E,
6
9Lv"q5]5!^`rmW!(R6; ) .8x-m
uR:9v, }7N\ [I oH1'hR] œ0, C z g Sf yd @Q<7 mo! Q V A
E4 !tB Gt=J`*-Yn>2/□H1:l's~G` ~Dm5bu?a b M @<-+2Aa
$
cU6r
'fu9
m" t,8l-w eB 96rzQφk E Wd4fwFL^ \kIq ( +4VVNε&(
4a[]s 輻 (
+rpT<u< "y$ PEK
eá v H' d< ) h2 : ?XVw A \
ka; E=eφ m n M ( , i H J 0 e - + # , ! r # D
? 5uN
b W Sa 薨 <2n l < N < L w Jwu || 7W
D. r d Qh: k > z z (% HG7 -
C M l a f ) B # U 9 3 , ? ? * 3 V 7
e % C PC x T
en B z Q $ @ d Z 9 ] ! ty W v ' H a O
4 \
i G P % l X 6 N k [ n j s Q R m n \
t R TWB < X $ T g J * y 2 z d 0 A * ^ H , F C I B ^ E c M M m
4 Y : H $ r Q w d R ) @ b * Q Z z 8 a \ ] o , : k > x o e I ; f f H ] 媿 g u h 8 P U ( R \ Z
) ! T W t . ? < * b / ] 6 A ) X 4 | Y i y { < h 0 < M h O w
# { T ( 0 7 4 D Z " | K B J | ' T R U u l . O B ; g Y o l { Y u F G d f M P G
```

Örnek Olay İncelemesi

Conti Ransomware’i kullanan her bir affiliate’ın ayrı bir hesabı olduğu ve farklı kurbanlara ait dataların bu sunucuda saklandığı görülmüştür.

- `sftp RLDASSOC@91.193.181.22 : epai5leba4aedah7ti - port: 1021`
- `sftp casin@91.193.181.22 : ua2nuohohCheiriex6 - port: 1021`
- `sftp PSB@91.193.181.22 : moR5oobohbutuis2ea - port: 1021`
- `sftp VNEURON@91.193.181.22 : ohka3oong5oDahsae7 - port: 1021`
- `sftp TRANZ@91.193.181.22 : naek2eiko6Aetahfai - port: 1021`
- `sftp coldtech@91.193.181.22 : Ue6pheengeiBuwo8ee - port: 1021`
- `sftp test@91.193.181.22 : mod2me6ahChoosu2ee - port: 1021`
- `sftp NEW@91.193.181.22 : aethoothei9uip5aXe - port: 1021`
- `sftp PSB@91.193.181.22 : aiteifoethoh0phooZ - port: 1021`
- `sftp AZCO@91.193.181.22 : Ra1uo3jae1Huopees4 - port: 1021`
- `sftp PSB@91.193.181.22 : 1L3soongaeH5eequai - port: 1021`
- `sftp EUNIVER@91.193.181.22 : noa3nei6poMeizaiYe - port: 1021`
- `sftp AIRMAR@91.193.181.22 : Obiejei5gaeSabahmi - port: 1021`
- `sftp choc@91.193.181.22 : chae2Phoochi6aiChe - port: 1021`
- `sftp DSC@91.193.181.22 : tohxaehir7haiquaYe - port: 1021`
- `sftp weconnect@91.193.181.22 : Neloshaephiph2kaja - port: 1021`

```

root@e20178:~# cat sftp_users

sftp testuser@91.193.181.22 : - port: 1021

sftp testuser2@91.193.181.22 : Ahgae8waefie9eiDe0 - port: 1021

sftp gold@91.193.181.22 : to7Noong8ao7ix4woe - port: 1021

sftp NUTCO@91.193.181.22 : thao8otee4Efoo9ahl - port: 1021

sftp TWB@91.193.181.22 : aimeisaeLe8ohePee9 - port: 1021

sftp teico@91.193.181.22 : ootheiFaaha4theemo - port: 1021

sftp ILS@91.193.181.22 : Aif7eu4fielIWajeiv - port: 1021

sftp concord@91.193.181.22 : Teequahjik5eiDi7ae - port: 1021

sftp idmuae@91.193.181.22 : ohveingohvait4EeKi - port: 1021

sftp AREA@91.193.181.22 : oor2teeM3iRlbeetai - port: 1021

sftp DUNA@91.193.181.22 : eengeephohv8Aimeeg - port: 1021

sftp UPS@91.193.181.22 : goat2to9ahsh2HeeJe - port: 1021

```

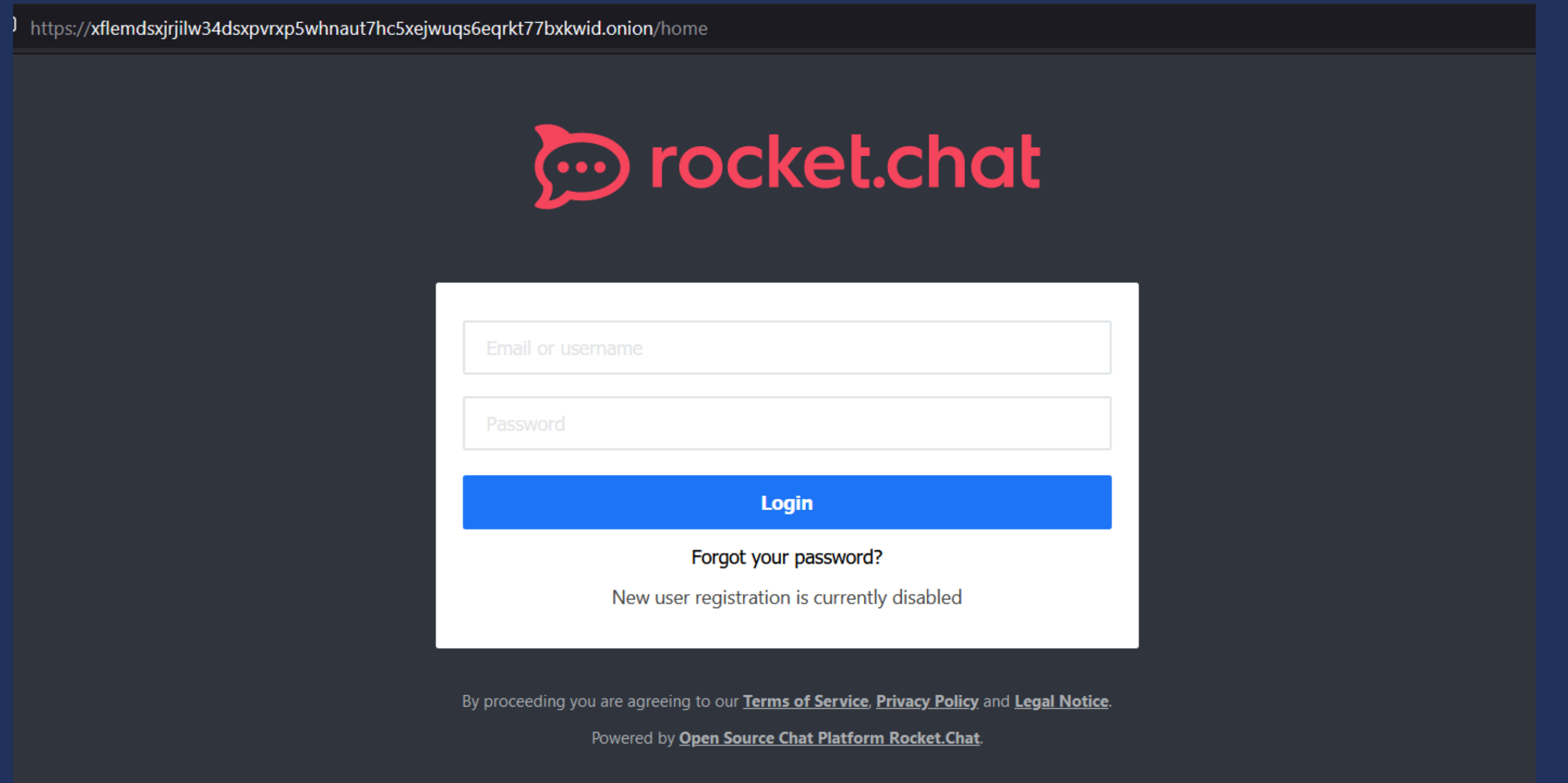
Örnek Olay İncelemesi

Devam edilen incelemelerde Conti'nin Rocket Chat sunucusuna ait bir kullanıcı giriş bilgisi tespit edilmiştir.

```
contiv2/185.25.51.173-20200715.json
5645: "body": "https://scrytnuuszglaugg.onion/login\nbotadmin / D347uk3d!"

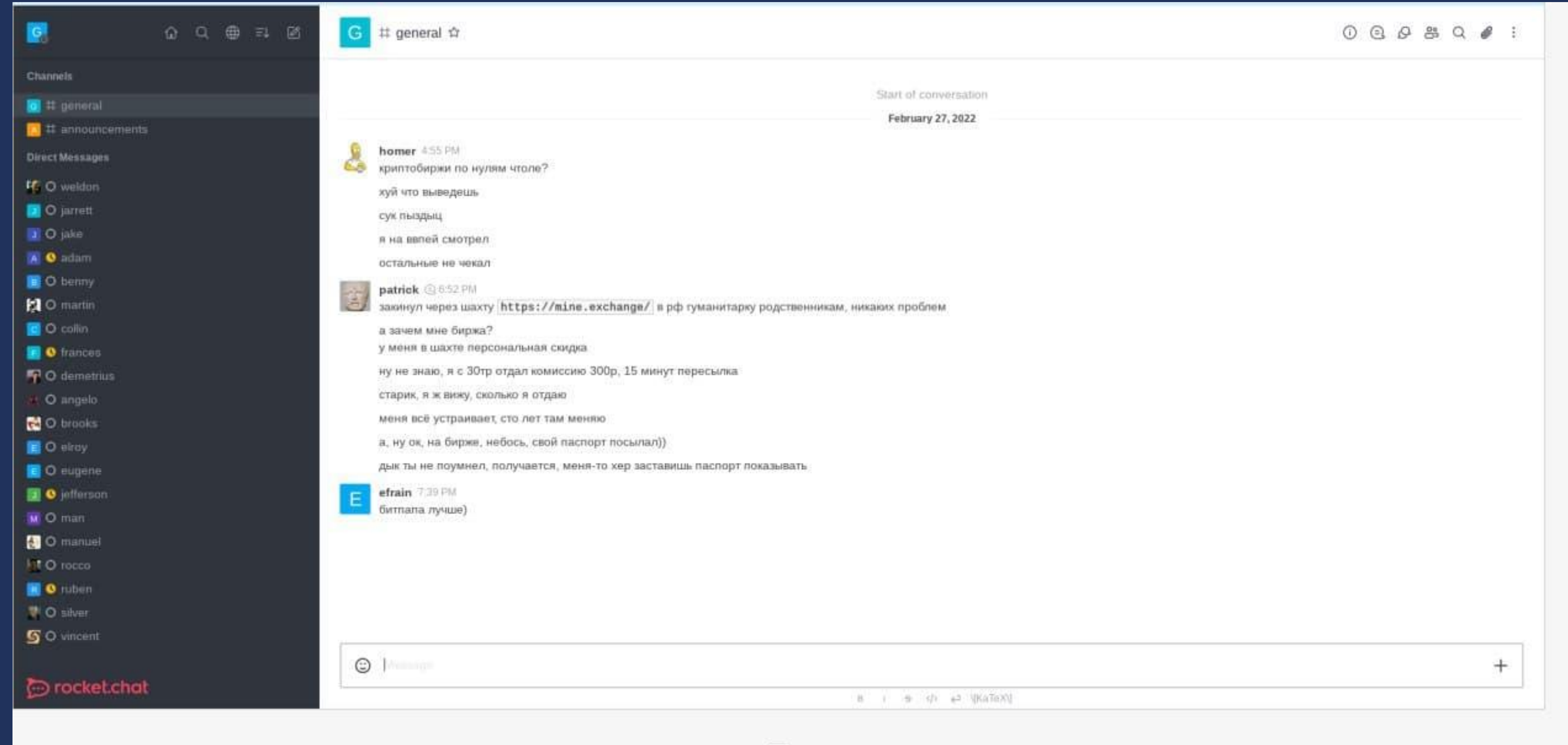
contiv2/185.25.51.173-20200709.json
1127: "body": "\n\nhttps://scrytnuuszglaugg.onion\nbotadmin:D347uk3d!"

contiv2/185.25.51.173-20200907.json
4025: "body": "ты когда мне botadmin"
4115: "body": "Даш новый пароль к botadmin?"
```



Örnek Olay İncelemesi

Conti Ransomware'ı kullanan toplamda 182 farklı ilişkili tehdit aktörü tespit edilmiştir.



Örnek Olay İncelemesi

Sızdırılan loglar incelenmeye devam edildiğinde bir kullanıcı hesap bilgisi tespit edilmiştir. İlgili panele giriş yapıldığında Bazar zararlı yazılımına ait bir C2 (command-and-control) sunucusu olduğu görülmüştür.

```
contiv2/185.25.51.173-20200715.json
5645: "body": "https://scrytnuuszglaugg.onion/login\nbotadmin / D347uk3d!"

contiv2/185.25.51.173-20200709.json
1127: "body": "\n\nhttps://scrytnuuszglaugg.onion\nbotadmin:D347uk3d!"

contiv2/185.25.51.173-20200907.json
4025: "body": "ты когда мне botadmin"
4115: "body": "Даш новый пароль к botadmin?"
```

Örnek Olay İncelemesi

Backdoor
Server time: 20:46:09 UTC
botadmin

- Dashboard
- Settings
- Administrators
- Bots
- Honeypots
- Test Bots
- Important
- Plugins
- Networks
- Network Activity
- TaskList
- Groups
- Files
- Proxies
- Reports

bots

Home > bots

Command Builder

Command Type: No Operation Timeout: 1 min

GO!

Advanced search options

Showing 821-840 of 3,705 items.

With selected
Run Command
Autorefresh 5 min

ID	Bot	Os	Group	Country	Ip	Domain	Hostname	First activity	Last activity	Status	Priority	Comment **	Actions
10167	be18ae57b1031831b36da6ced330daa0	g15	IN	43.250.157.90	CYPRESSINDUSTRI	CIPL198	2021-12-21 02:40:50	2022-01-24 18:06:05	offline	*	Shved test		
9434	4111115006101090811027442137883862184696	g15	US	71.233.64.217	ultra-ussi.com	JDELLI21-LT	2021-12-13 12:06:00	2021-12-13 16:05:59	dead	*	Shved test		
10939	52bc43bac07305b778ab9470cc647b63	g15	IN	202.131.123.12	SERVER7	PCT98	2022-01-13 19:09:36	2022-01-29 20:48:03	online	*	Shved work		
599	0129706482725354735054636025741101228607	25	US	47.206.124.216	apg.local	WHITIM1	2021-11-03 12:44:36	2021-12-17 23:13:27	dead	*	Shved work		
10053	2914611297171653887710177438123182158785	25	US	172.241.224.132	nfadm.local	NFADM-1355	2021-12-17 17:18:55	2021-12-22 22:22:06	dead	*	small		
11770	bc5c58bc3c2bfc7caf145b83f5f6bd0	57	US	208.125.241.250	RTC	RICH2021	2022-01-25 14:02:42	2022-01-26 14:13:37	offline	*	SMOTRET		
344	94cf76ff182338a4cee6254dd8a288	19r	US	72.28.227.166	WORKGROUP	DRMASSIE-HP	2021-11-02 15:38:57	2021-11-11 00:27:59	dead	*	as in work		
7869	0cebce62b19b7e2f1016439187b997b7	g11	US	47.206.94.203	CDSOFFICE	SUPPORT12	2021-11-30 16:08:44	2022-01-29 20:47:15	online	*	STEVE		
7779	6ab4bcb0187566f489ba5255375f7053	g11	US	50.250.43.57	CI	CI-D8	2021-11-30 18:41:02	2021-12-09 12:58:47	dead	*	STEVE		
8501	ad14d54629be45f7bc214d6873f03f74	g11	US	108.215.202.177	PLASWFD1	PIA-LAP51	2021-12-03 15:55:28	2022-01-14 22:55:20	dead	*	STEVE		
7964	02b8abf218743bf6d05e1d6aa0f0de25	g11	US	209.64.33.114	KC	KC-O3050-AP	2021-12-01 16:07:28	2022-01-28 21:46:20	offline	*	STEVE		
8644	3d26b20370c18612ce297b8b63834f8b	g11	US	162.211.146.146	ALCLTD	ALC-TAYLORPOWEL	2021-12-03 18:10:04	2021-12-13 19:06:31	dead	*	STEVE		
7009	0172369541013127092542829638801660622620	g12	US	64.203.115.142	wbi.local	STATION10	2021-11-24 17:42:35	2021-12-15 01:54:04	dead	*	STEVE		
6492	0020817331414051504561730056394513858371	g12	US	163.150.160.4	yejusd.us	DECPURMGRW10	2021-11-22 20:05:19	2021-12-22 13:35:59	dead	*	STEVE School District		
5185	00096972252713405668835547551349671194135	g12	US	173.246.230.162	farrell.local	COF-WS-11	2021-11-16 21:09:55	2021-12-19 09:29:12	dead	*	STEVE Орган муниципальной власти		
11237	3926466958424961024533628251421797487654	g8	US	67.216.25.2	irvingtexas.local	ICVBG6UXQ7PJH6Y	2022-01-19 15:07:14	2022-01-20 02:12:54	dead	*	STV		
11112	3963285790264247388120345772601205434924	g8	US	131.94.122.155	eng.fiu.edu	EICAPPS5	2022-01-18 13:37:39	2022-01-18 20:25:12	dead	*	STV		
11074	0313240845387210851227407260921945253398	g12	US	70.185.88.75	us.gopaschal.com	SP-ITD2	2022-01-17 21:30:38	2022-01-19 22:04:29	dead	*	STV		
11172	1889033139420334559218264820321865722309	g8	US	71.199.175.93	MRC.local	MRC-00044	2022-01-18 21:56:00	2022-01-20 23:32:37	dead	*	STV		
11273	4246096033376420030013016761394228410420	g8	US	70.182.220.72	midtown.local	DALE-PC	2022-01-19 17:49:56	2022-01-26 13:05:35	offline	*	STV 14 host		

Örnek Olay İncelemesi

Backdoor
Server time: 20:45:57 UTC botadmin

- Dashboard
- Settings
- Administrators
- Bots**
- Honeypots
- Test Bots
- Important
- Plugins
- Networks
- Network Activity
- TaskList
- Groups
- Files
- Proxies
- Reports

bots
Home > bots

Command builder

Command Builder

Command Type Run .exe No Operation	Run type Process Hollowing	Timeout 1 min 1 min	Host Process notepad.exe Not use	Select/Upload execution file ...	Parameters
---	--------------------------------------	----------------------------------	---	--	-------------------

GO!

Process Hollowing
 Process Doppelganging
 CreateProcess

Advanced search options
Showing 601-620 of 3,705 items.

bots listing

With selected
Run Command
Autorefresh 5 min
All

ID	Bot	Os	Group	Country	Ip	Domain	Hostname	First activity	Last activity	Status	Priority	Comment	Actions
+ 8444	096ff7314388b2bc05ed9ed018ed57ed	64	g11	US	208.105.173.3	ITSNE	2020ROBVDI2	2021-12-03 15:26:13	2021-12-04 14:16:05	dead	*	DIL *rix IN WORK	
+ 10896	0222710546334308290914058062262254859170	64	g8	US	20.97.58.49	shmilyexpress.local	DESKTOP-AL22RAS	2022-01-12 15:40:56	2022-01-14 23:20:41	dead	*	DIL saawi	
+ 8650	209c9d873c03266f3a3691080bbd92af	64	g11	US	69.147.3.25	EISD	1120LAP181719TD	2021-12-03 18:12:23	2021-12-10 21:37:22	dead	*	DIL *SaaWi in work	
+ 11287	0032887713553224299292388758705275148993	64	g8	US	67.217.157.5	bps.local	5PBKS13	2022-01-19 18:39:57	2022-01-20 21:06:20	dead	*	DIL saawi team	
+ 2083	0151045043221893006981330283331488699351	64	g12	US	68.207.107.160	EPCHA.local	EPCHAWKS0120	2021-11-08 20:38:31	2021-11-12 15:56:37	dead	*	DIL seicas vne domena (skoree vsego vpn off)	
+ 5164	0307020124662413603137281418144128454922	64	g12	US	47.206.146.83	TBSC.local	RUTH-MID	2021-11-16 19:37:58	2021-11-23 18:18:37	dead	*	DIL srazy doxnet	
+ 5076	0036403918582076247515728941934040460289		g12	US	199.231.106.58			2021-11-16 16:58:02	2021-11-24 15:30:15	dead	*	DIL srazy doxnet	
+ 11393	0003974672332510376248270635823407761346	64	g8	US	50.127.151.7	bmh.org	THOPKINS	2022-01-20 15:47:18	2022-01-20 17:23:02	dead	*	DIL srazy ymerat	
+ 8576	a4811b23bfb6de0a32e579b51f3e0892	64	g11	US	98.37.76.33	CBKS	LOANER10--X260	2021-12-03 17:44:21	2021-12-08 01:44:27	dead	*	DIL *steve IN WORK	
+ 8458	b79cfe50efac45f06406cb394802d111	64	g11	US	52.44.244.137	cmdservice	EC2AMAZ-	2021-12-03 15:41:13	2021-12-22 13:38:53	dead	*	DIL *Steve_IN WORK	

Örnek Olay İncelemesi

CONTI.News 06:23

Your login

Your Password

SignIn

CONTI.Recovery Chats 21:58 bio1

Chat created
System message 2 days ago

<http://contirec7nchr45rx6ympez5rjldlbnqzh7ls>

OP

pepsi

Created at

2 days ago

Updated at

2 days ago

Online at

2 days ago

Name

Email

Domain

lyonwaugh.net

Comment


lyonwaugh.com
27 serv
1000 host
34g

Hide all messages

Ban ID Delete chat

SEND

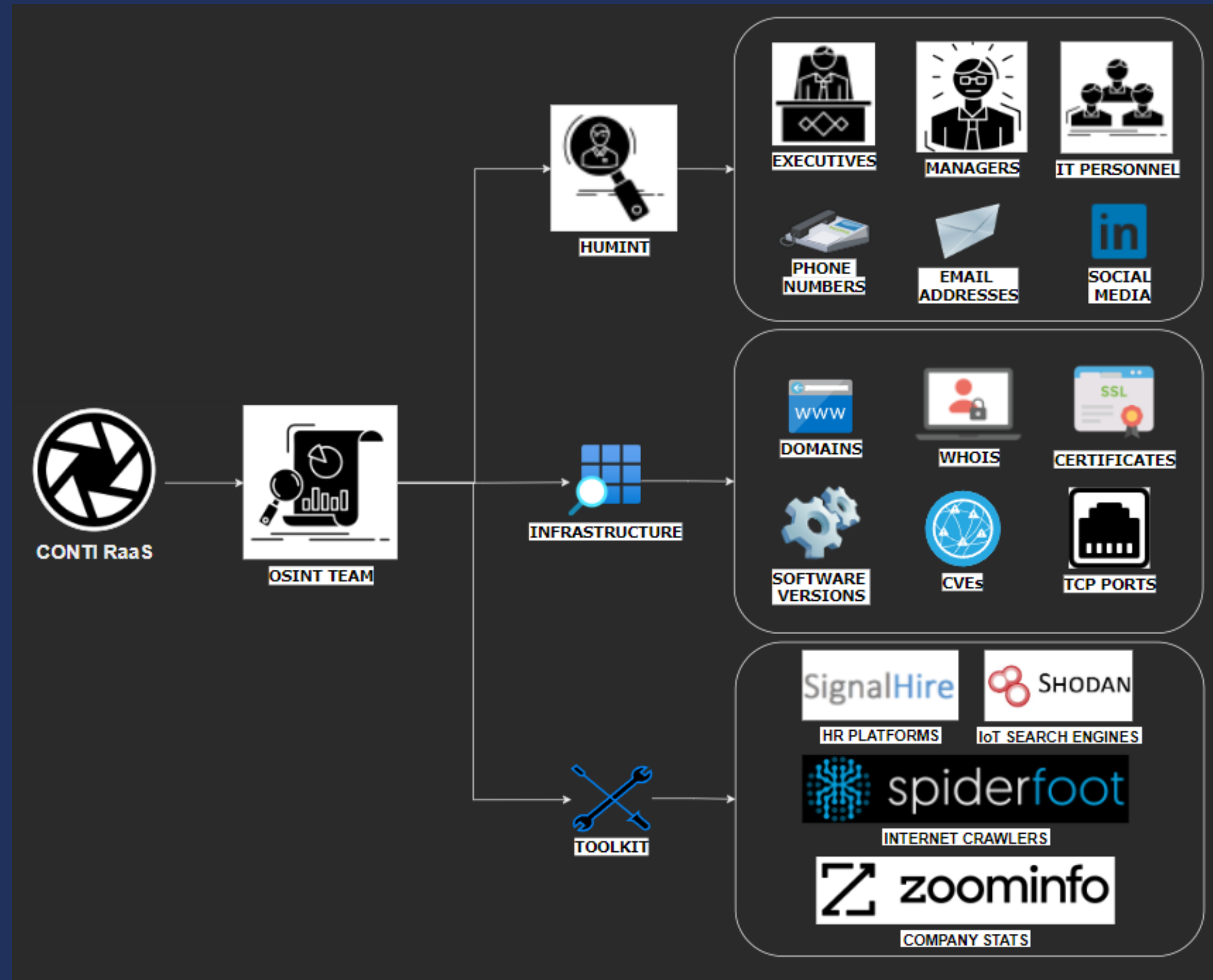
Örnek Olay İncelemesi

CONTI.Recovery  Chats 🕒 20:26 👤 bio1

Status All active Search Apply filter

ID	Domain	OP	Status	Updated at
ybDlfd1mzTBPYo5dyj6JZxMmDtmfJ10F4NJyOpQSiAjMHstTJGMe570USnFTRSM	WINNAVEGAS	icen	Wait answer	22 hours ago
UZeMXpgTHd6cxJuArkXwHbRhLfAcC6hyiZh70jFwZuoqf14EvbfhDZETNIM8mu8H	LAVI	icen	Repled	5 days ago
PDUjTpuDovNaXeb01e2bZRldfXH8QTreggpulWu03iHd9w2hAHpldLxOtoYoQhFo	RLDASSOC	icen	Repled	6 days ago
Hgdna5MEV4I2YJfbtPQyquzEOJ06BRPhhtUmfDYSVVj67ZYXQD3MaUtpPa2rGqjI	TRANZ	icen	Wait answer	7 days ago
otcpa5UckEz6hoEa7hld1fY2OLmo2s84PrqqJrHRSaWaYR6Z4tZsLlqfHza3tfn8	AEE	icen	Repled	15 days ago
O34WUyhBlvw4cb4dUR8NTbZULwX5LuEJCUZrtbLMZUh2p8wcbKsIPcV7hRTCQaDr	TCEC	icen	Repled	20 days ago

Conti Cyber Kill Chain



İstihbarat Bulgularını Raporlama

İstihbarat Bulgularını Raporlama

- Terminoloji ve önemli anahtar kelimelerin açıklanması,
- İstihbarat bulgusunun hangi sektörü ve kimleri etkilediği,
- Bulguyu inceleyecek, raporu analiz edecek ekiplerin belirtilmesi,
- İstihbarat bulgusunun etkileri,
- İstihbarat bulgusunun kaynağı,
- Kullanılan araçların belirtilmesi ve açıklanması,
- Aksiyon alınabilir veri sunulması.

İstihbarat Bulgularını Raporlama

Apt Groups Report Template Dependency

Mission and Vision, Historic Background

Country and Industries Target Map

Activities/Operation List by Year

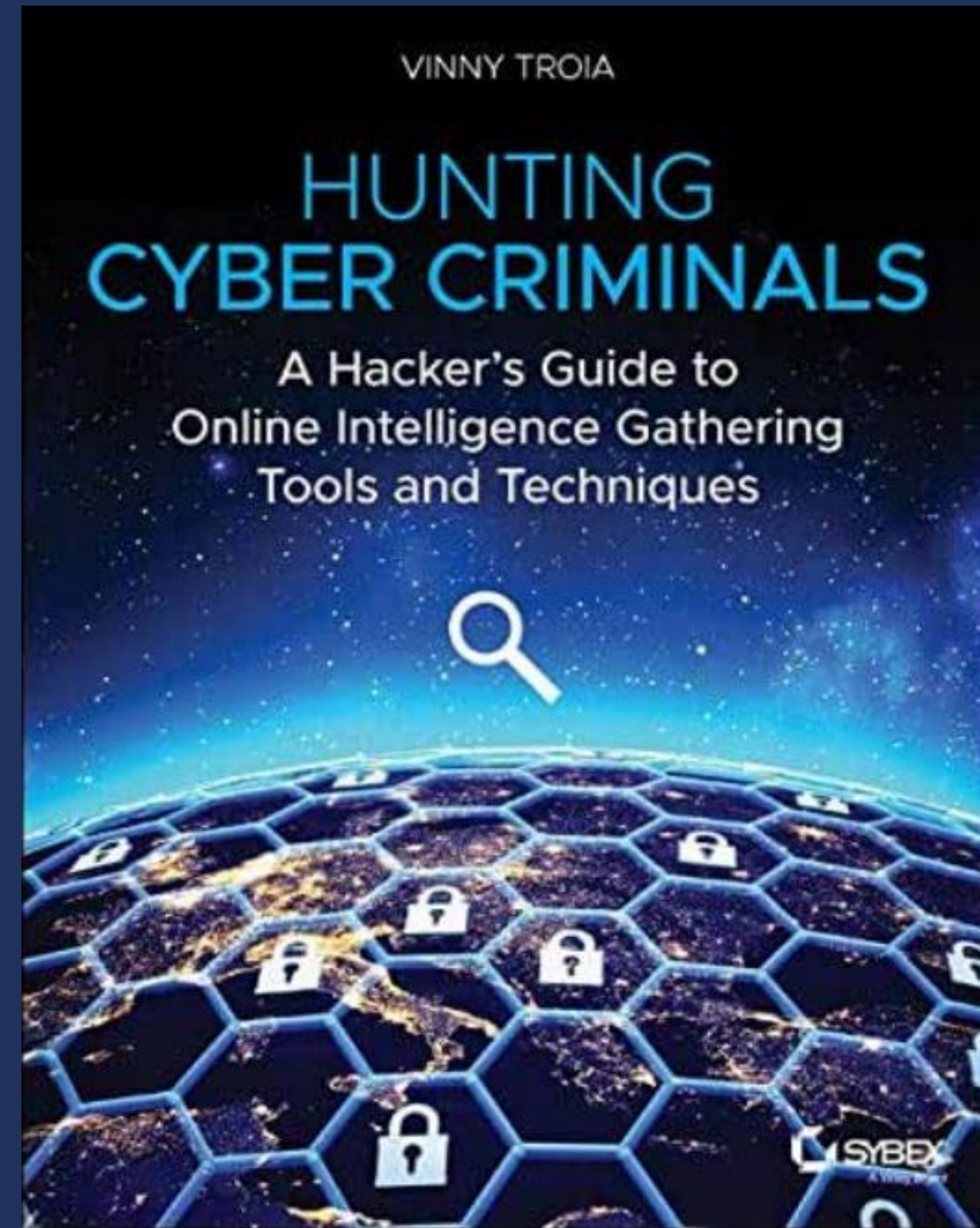
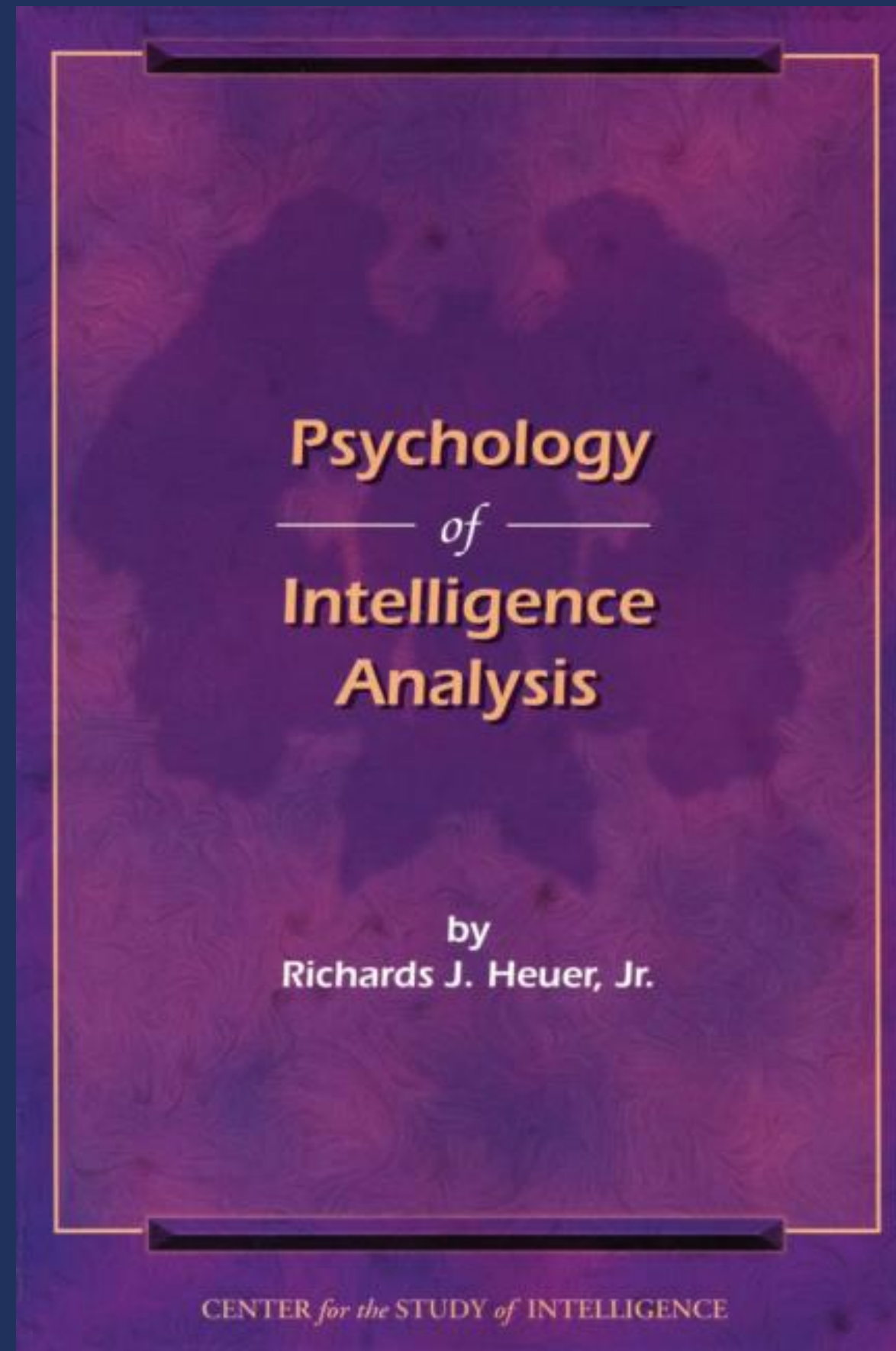
Attack LifeCycle, TTPs

Toolsets and Related Malwares

IoC, Recommendations and Outlook

Ek Kaynak / Öneri

Must Read



Build Up!

Threat/Warning Analyst Work Role ^

(AN-TWA-001)

Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.

- Abilities
- Knowledge
- Skills
- Tasks
- Capability Indicators

CTI Bookmarks

<https://map.malfrats.industries/>

<https://osint.link/>

<https://darkfeed.io/>

<https://www.vx-underground.org/index.html>

<https://inteltechniques.com/blog/>

<https://start.me/p/ZME8nR/osint>

<https://github.com/rshipp/awesome-malware-analysis>

Teşekkürler.
