



AÇIK KAYNAK KODLU SİBER TEHDİT İSTİHBARATI ÇÖZÜMLERİ

Yazar: Samet Sazak

Baskı: 2018

İÇİNDEKİLER:

MISP - Open Source Threat Intelligence Platform	3
YETI - Your Everyday Threat Intelligence	4
Yeti Kullanım Alanları	5
Cuckoo Sandbox.....	6
Analiz:.....	7
Raporlama:	7
Collective Intelligence Framework	8
CIF Nasıl Çalışır?	9
Abuse.IO.....	10
Abuse.IO ana özellikleri:	10
Abuse.IO içerisinde bulunan parserlar ve kaynakları.....	11
stoQ - Analysis Simplified	12
Stoq Nasıl Çalışır?	12
Ingestion Aşaması	12
Zenginleştirme	13
İşleme.....	13
Export.....	13
TekDefense - Automater	14
Kullanımı:.....	14
Forager.....	15
Özellikler:.....	15
GOSINT Framework.....	16
Loki IOC Scanner	17

MISP - Open Source Threat Intelligence Platform



MISP (Zararlı Yazılım Bilgi Paylaşım Platformu) siber tehdit istihbaratının paylaşımına yardımcı olan ücretsiz ve açık kaynak kodlu bir projedir.

MISP, hedeflenen saldırıların, mali dolandırıcılık bilgilerinin, güvenlik açıklarının veya terörle mücadele bilgilerinin ele geçirilmesi ve toplanması, paylaşılması, depolanması ve ilişkilendirilmesi için oluşturulmuş bir siber tehdit istihbaratı platformudur.

MISP platformu kurum ve kuruluşların zararlı yazılım tehdit göstergeleri (malware IOCları) hakkında bilgi paylaşmalarını sağlar. Kullanıcılar, zararlı yazılımlar (malware) veya tehditler hakkındaki "iş birliğine" dayalı bilgiden yararlanırlar. Bu güvenilir platformun **amacı**, hedeflenen saldırılara karşı kullanılan karşı önlemlerin geliştirilmesine yardımcı olmak ve önleyici eylemler oluşturmaktır.

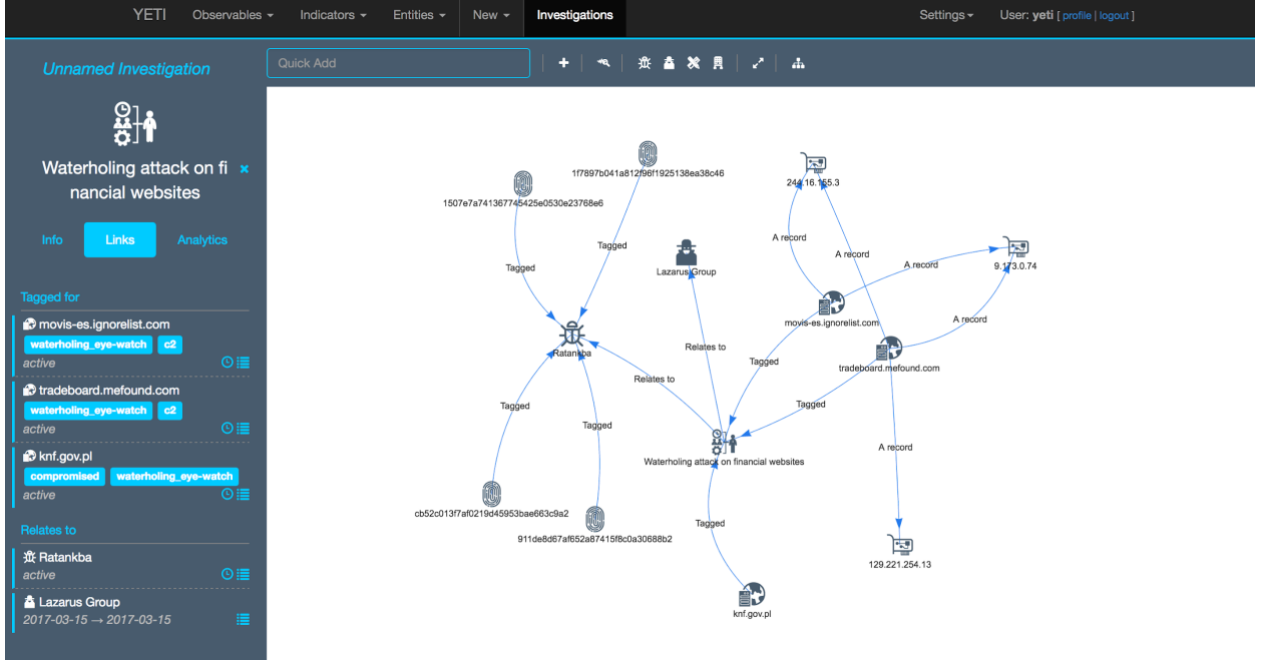
MISP, bir web ara yüzü (analistler veya olay müdahale ekipleri için) üzerinden kullanılabilir. Bir REST API üzerinden de tehdit göstergelerini (IOCs) alıp gönderebilir. MISP platformunun temel hedefi tehdit bilgilerini açığa çıkarmayı, olgunlaştırabilmeyi ve istismar edilmesini önleyen sorunsuz bir operasyon sağlayan sağlam bir platform olmaktır.

Proje: <http://www.misp-project.org/>

Github: <https://github.com/MISP>

Topluluk: <http://www.misp-project.org/communities/>

YETI - Your Everyday Threat Intelligence



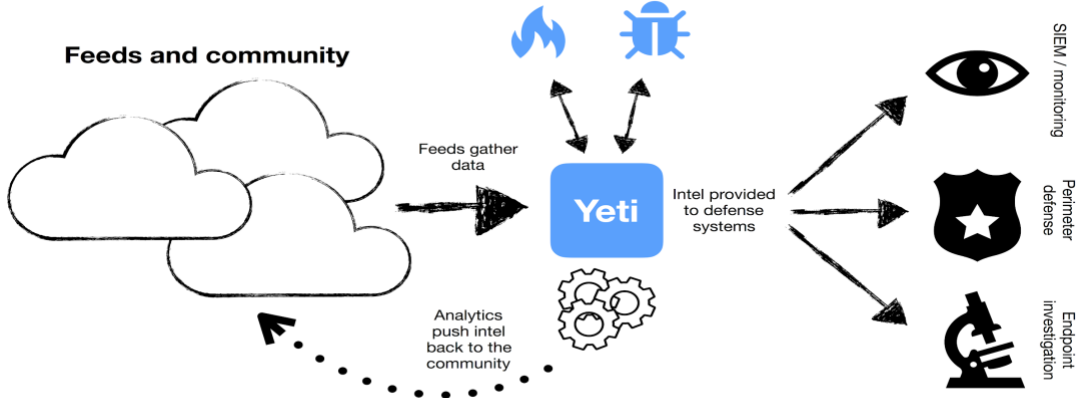
Yeti, tehdit göstelerini (indicator of compromise) ve bu göstergelerin teknik, taktik ve prosedürleri (TTP) hakkındaki bilgileri tek bir depoda organize etmeyi amaçlayan bir platformdur.

Yeti, tehdit göstergelerini (IOC) otomatik olarak zenginleştirebilme özelliğine sahiptir. Örneğin domain alanlarını çözmek, IP adreslerini coğrafi konumlara ayırmak gibi. Yeti kullanıcıların rahat bir ortamda çalışabilmesi için “Bootstrap” tabanlı bir kullanıcı ara yüzü sunmaktadır. Bir web API arabirimi üzerinden diğer araçlarla entegre edilebilmekte ve kullanılabilir.

Yeti, çok çeşitli kaynaklardan örneğin yazımızda bahsettiğimiz zararlı yazılım bilgi paylaşım platformu olan MISP üzerinden zararlı yazılımlara ait göstergeler, XML özetleri, JSON verileri toplayabilir ve işleyebilmektedir. Sorguları otomatik hale getirebilir ve olay müdahale ekiplerinin işlerine yardımcı olabilmektedir. Yeti, yakın zamanda piyasaya sürülen ve tehdit istihbarat yönetimini kolaylaştırmayı amaçlayan birçok araçtan biridir. Beslemeler ile verilerini derlemenize ve zenginleştirmenize yarayacak çok geniş bir araç kombinasyonuna sahiptir.

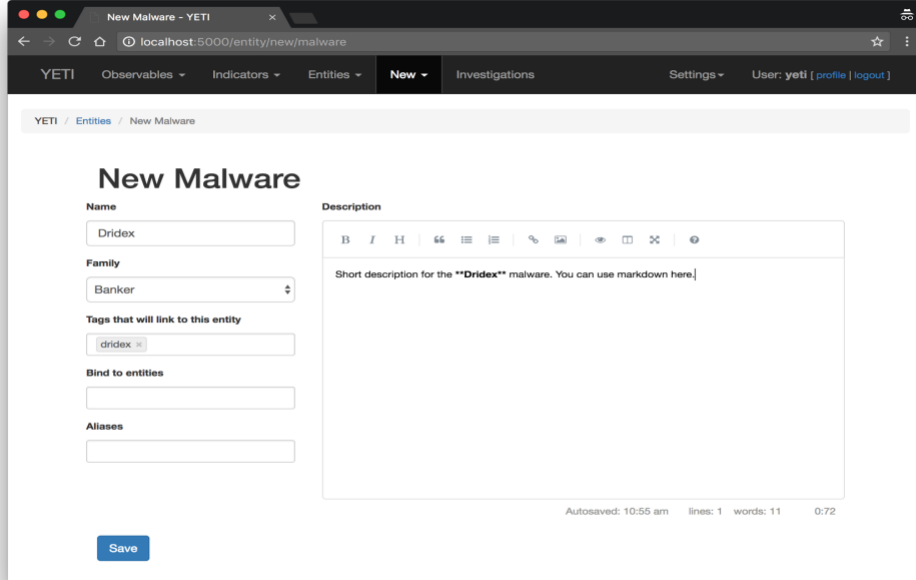
Yeti üzerine eklenen tüm bu verileri hızlıca listeleyebilir, analiz edebilir, ilişkilendirebilir ve dışa aktarım sağlayabilirsiniz. Örneğin bu veriler SIEM gibi ürünlere meşhur formatlarda aktarılabilir ve entegrasyon sağlanabilir. Bu sayede yapılan analizler sonucu bulunan tüm bulguları SIEM gibi yazılımlar üzerine aktarmakla uğraşmaktan kurtarmaktadır.

[AÇIK KAYNAK KODLU SİBER TEHDİT İSTİHBARATI ÇÖZÜMLERİ]



Yeti Kullanım Alanları

Örneğin zararlı yazılımları tespit edebilmek için bir sandbox sisteminiz var ve yeni bir bankacılık zararlısı tespit ettiniz. Bu zararlı yazılım çaldığı verileri depolamak için kullanıcının "Roaming" dizininde başka bir alt dizin kullandığını anladınız. Bunu belgellersiniz ve böylece başka bir analist bu davranışı gördüğünde bunun bir bankaları hedefleyen bir zararlı yazılım davranışı olduğunu kolayca tespit edebilmesine yardımcı olabilirsiniz.



Web: <https://yeti-platform.github.io/yeti-ecosystem>

Github: <https://github.com/yeti-platform/yeti>

Topluluk: <https://yeti-platform.github.io/community>

Cuckoo Sandbox



Cuckoo Sandbox, şüpheli dosyaların analizini otomatikleştirmek için kullanabileceğiniz açık kaynaklı bir yazılımdır. Bunu yalıtılmış bir ortamda çalışırken, "zararlı işlemlerin davranışlarını" izleyen özel bileşenlerden yararlanmaktadır.

Şüpheli herhangi bir dosyayı birkaç dakika içinde sandbox ortamına yükledikten sonra Cuckoo bu dosyayı gerçekçi ancak yalıtılmış bir ortamda yürütür daha sonra size bu dosyanın davranışını özetleyen ayrıntılı bir rapor sunmaktadır.



Info	File	Signatures	Screenshots	Static	Dropped	Network	Behavior
Category	Started On	Completed On	Duration	Cuckoo Version			
FILE	2013-01-26 23:50:42	2013-01-26 23:53:10	148 seconds	0.5			

File Details file indicators

File name	efeb717fdbb98d8043eb4c51254d9b74
File size	93696 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
CRC32	83427EDE
MD5	efeb717fdbb98d8043eb4c51254d9b74
SHA1	2644a7c50aa3cd366be0dd219efe531ed72ae514
SHA256	8dafb21e7d106a6c98f745f30c2577ee7b0984ec7ba2c4107f7ddcd0d127baf6
SHA512	097e682a4723c6e72caaac01e49711b21e8091cdbcab90a192aa233b8a9e0ef3c4468951f4f53falb6543d55395c6e6859c2a6b121d697cc7489d570d623273
Ssdeep	None
PEID Signatures	None matched
Yara Signatures	
Antivirus	38/42 (collapse)

Analiz:

Windows, Linux, Mac OS X ve Android sanal ortamlarında zararlı web sitelerinin yanı sıra birçok farklı zararlı dosyayı (çalıştırılabilir dosyalar, ofis belgeleri, pdf dosyaları, e-postalar vb.) analiz etmenizi sağlamaktadır.

- API çağrılarını ve dosyanın genel davranışını izleyebilir hale getirmekte ve bunu herhangi bir kişi tarafından anlaşılabilir olan üst düzey bilgi ve imzalara dönüştürebilmektedir.
- SSL / TLS ile şifrelenmiş olsa bile ağ trafiğini analiz edebilmenizi, yerel ağ yönlendirme desteğiyle, tüm trafiği kesebilir, InetSIM veya ağ arabirimi veya VPN aracılığıyla yönlendirebilirsiniz.
- Enfekte edilmiş sanallaştırılmış sistemin gelişmiş bellek analizini, Volatility ile birlikte YARA'yı kullanarak bir process memory parçacığı üzerinde çalışabilmektedir.

Cuckoo'nun açık kaynak niteliği ve kapsamlı modüler tasarımı sayesinde analiz ortamının, analiz sonuçlarının işlenmesinin ve raporlama aşamasının herhangi bir yönünü özelleştirebilirsiniz. Cuckoo, sandbox'ı istediğiniz framework'e istediğiniz şekilde, istediğiniz formata lisanslama gereklilikleri olmadan kolayca entegre etmek için tüm gereksinimleri sağlar.

Raporlama:

Cuckoo, Zararlı yazılım izleme sonuçları ve davranışlarının ayrıntılı açıklamalarını içeren büyük log dosyaları (örnek olarak ortalama 6 MB, ancak 100 MB'ye ulaşılabilir) oluşturur. Cuckoo kullanarak topladığımız veriler şunları içerir:

- API logları
- Network(Ağ) Logları
- Drop edilen dosyalar hakkında statik veriler
- Ekran görüntüleri
- Sistem manipülasyonu: Dosyalar / Kayıt / Mutexler / Hizmetler
- Başlangıç processleri ve örneklerle ilişkileri

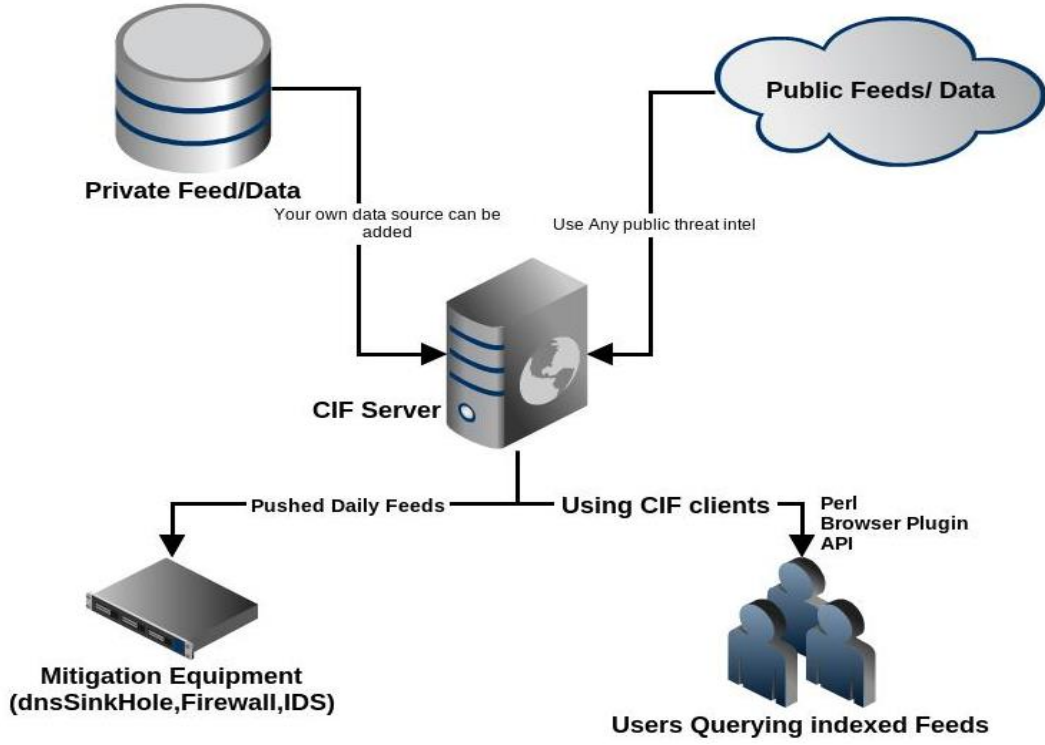
Bu bilgilerle, örnekleri davranışlarına göre sınıflandırmak mümkündür. Zararlı yazılım tanımlamaları oluşturmak ve zararlı yazılım bulaşmalarının çoğunu düzenlemek için de yeterli bilgi sağlamaktadır.

Web: <https://cuckoosandbox.org/>

Github: <https://github.com/cuckoosandbox>

Dokümantasyon: <https://cuckoo.sh/docs/>

Collective Intelligence Framework



CIF, bir siber tehdit istihbarat yönetim sistemidir. CIF, birçok kaynaktan gelen bilinen zararlı yazılım tehdit göstergelerini (IOC) birleştirmenize ve bu bilgileri tanımlamanızı ve algılamanızı sağlamaktadır. CIF'te depolanan en yaygın tehdit göstergeleri türleri, zararlı etkinlikle ilişkili olduğu gözlenen IP adresleri, FQDN'leri ve URL'lerdir. CIF, çeşitli tehdit verilerini herhangi bir kaynaktan alabilmektedir. Framework'ün çalışma mantığı şu şekildedir.

- Herhangi bir kaynaktan veri alma.
- Bu veriyi kaydetme ve reputation(itibar)'a göre değerlendirme.
- Sorgular aracılığıyla tekrar veriye erişim ve dışarı aktarma.

CIF Nasıl Çalışır?

Parse (Ayrıştırma Süreci)

CIF, aynı tipteki birçok farklı veri kaynağından veri toplamayı destekler; Örneğin, zararlı domainlerin veri setleri veya feedlerini (beslemeleri) toplayabilir. Her benzer veri setini kaynak veya güvenilirlik oranı gibi farklı niteliklerle işaretlenebilmektedir.

Normalize (Normalleştirme)

Tehdit istihbaratı veri setleri genellikle aralarında ince farklara sahiptir. CIF, diğer uygulamalarda veya süreçlerde tehdit istihbaratından yararlanırken size öngörülebilir bir deneyim sunan bu veri kümelerini normalleştirmektedir.

Post Process

CIF, tek bir tehdit istihbaratından ek istihbarat elde eden birçok işlemciye sahiptir. Basit bir örnek, bir domain ve bir IP adresinin CIF içine alınan bir URL'den türetilmesidir.

Store (Depolama)

CIF, milyonlarca tehdit istihbarat verilerini depolamak için son derece optimize edilmiş bir veritabanı şemasına sahiptir. CIF v2, Elasticsearch kullanmaktadır.

Query (Sorgu)

CIF bir web tarayıcısı, yerel istemci veya doğrudan API kullanılarak sorgulanabilmektedir. CIF, milyonlarca kayıt veritabanına karşı sorgulama yapmak için son derece optimize edilmiş bir veritabanı şemasına sahiptir.

Share (Paylaşma)

CIF kullanıcıları, grupları ve api anahtarlarını destekler. Her tehdit istihbaratı verisi, belirli bir kullanıcı grubuyla paylaşılacak üzere etiketlenebilir. Bu, tehdit istihbaratının federasyonlar arasında paylaşılmasına izin vermektedir.

Produce

CIF, depolanan tehdit istihbaratından yeni veri kümeleri oluşturulmasını destekler. Bu veri setleri, tür veya güvenilirlik ile oluşturulabilir. CIF ayrıca feed oluşturma sürecinde whitelisting desteklemektedir.

Proje sitesi : <http://csirtgadgets.org/>

Github: <https://github.com/csirtgadgets/massive-octo-spice>

Abuse.IO

AbuseIO, (kötüye kullanım/suistimal) raporları almak, işlemek, ilişkilendirmek ve ağınızdaki suistimal vakaları ile ilgili belirli bilgileri içeren bildirimleri oluşturmak ve göndermek için kullanılabilecek, açık kaynak kodlu ve ücretsiz bir araç setidir. AbuseIO'nun amacı, suistimal süreçlerini otomatikleştirmek ve geliştirmektir.

```
abuseio@ar3:/opt/abuseio$ php artisan user:list
```

ID	Account	User	First Name	Last Name	Roles
1	Default	admin@isp.local	System	Admin	System Administrator
2	Default	user@isp.local	Elizabeth	Smith	Abusedesk User
3	Customer Internet	admin@isp2.local	Warren	King	System Administrator
4	Customer Internet	user@isp2.local	Sophie	Davidson	Abusedesk User
5	Business Internet	admin@isp3.local	Richard	Paterson	System Administrator

```
abuseio@ar3:/opt/abuseio$ php artisan ticket:list
```

Id	Ip	Domain	Class id	Type id
1	172.16.10.13		BOTNET_INFECTION	ABUSE
2	fd1:cb9d:f59e:19b0:0:45:0:22		BOTNET_INFECTION	ABUSE
3	10.0.2.150		COMPROMISED_SERVER	ABUSE
4	fd1:cb9d:f59e:19b0:0:33:4f		COMPROMISED_SERVER	ABUSE

Abuse.IO ana özellikleri:

- Abuse mesajlarını alıp abuse raporlarına otomatik olarak parse etmek ve mail yoluyla iletmek (bir posta sunucusu işleyicisi, örn. Postfix aracılığıyla)
- Karmaşıklığı azaltmak için zaten açık bir durumda olan raporları birleştirilebilir,
- Abuse türlerini sınıflandırmak ve belirli vakalarda özel eylemler oluşturabilir,
- IPAM sisteminizi kolayca entegre edilebilir,
- Case(olay) başına otomatik bildirimler ayarlanabilir,
- Olayları yanıtlama, kapatma veya not ekleme, organize olmalarını sağlamaktadır

New event CSV Export

Show 10 entries Search: 10.0.2

Ticket Id	IP	Domain	Type	Classification	Events	Notes	Status
3	10.0.2.150		Abuse	Compromised server	1	0	Open
9	10.0.2.100		Abuse	Copyright Infringement	1	0	Open
37	10.0.2.23	nacions.com	Abuse	Compromised website	3	0	Open
38	10.0.2.26		Abuse	Phishing website	2	0	Open
48	10.0.2.2		Abuse	Compromised website	1	0	Open

Abuse.IO içerisinde bulunan parserlar ve kaynakları

- Any RFC compliant ARF formatted message
- Any RFC compliant FBL Messages (Feedback Loop)
- Any DNS based RBL
- Shadowserver (www.shadowserver.org)
- SpamCop (www.spamcop.net)
- IP Echelon (www.ip-echelon.com)
- fail2ban reporting service (www.blocklist.de)
- Junk Email Filter (www.junkemailfilter.com)
- Google Safe Browsing reports for ASN's (safebrowsingalerts.googlelabs.com)
- Project Honey Pot (www.projecthoneypot.org)
- Clean MX (<http://www.clean-mx.de>)
- Cyscon / C-SIRT (<https://www.c-sirt.org>)
- Netcraft (<http://www.netcraft.com/>)
- SpamExperts (<https://www.spamexperts.com>)
- USGO-Abuse
- Microsoft SNDS
- Abuse-IX (<https://www.abuseinformationexchange.nl/>)
- Woody (<http://www.woody.ch/>)
- Webiron (<https://www.webiron.com/>)
- Copyright Compliance
- Cegtek (<http://www.cegtek.com/>)
- Juno (<http://www.juno.com/>)

Web: <https://abuse.io/>

Github: <https://github.com/AbuseIO/AbuseIO>

Blog: <https://abuse.io/blog/>

stoQ - Analysis Simplified



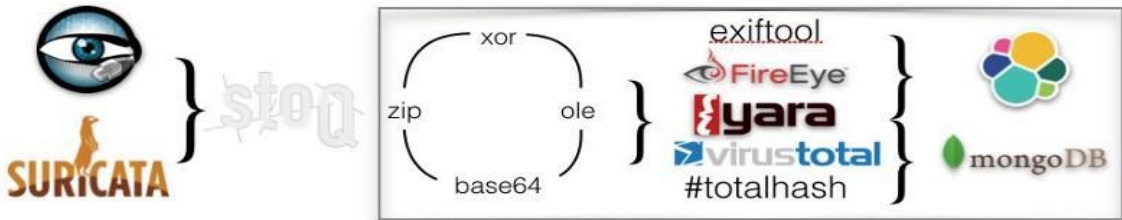
stoQ, bir analistin yapması gereken daha sıradan ve tekrar eden görevleri basitleştirmeye yardımcı olan bir otomasyon frameworküdür. Analistlerin ve DevSecOps takımlarının farklı veri kaynaklarından, veritabanlarından, decoder/encoderlardan ve diğer birçok görevden hızla geçiş yapmalarına olanak tanır. stoQ, bireysel güvenlik araştırmacıları için yeterince kullanışlıdır. Ayrıca kurumsal hazır ve ölçeklenebilir olacak şekilde tasarlanmıştır.

StoQ Nasıl Çalışır?

Temel olarak stoQ, bir analistin iş akışının (workflow) ortasında olacak şekilde yapılandırılmıştır.

Ingestion Aşaması

stoQ verileri tek tek dosyalardan alabilir, yeni dosyaların oluştuğu bir dizini izleyebilir, bir veritabanından veya bir API'den alabilir. Bu ölçekte stoQ'nun son derece güçlü olduğu yer burasıdır. HTTP veya e-posta gibi tehdit vektörlerinden dosya ayıklamak, otomatik zenginleştirme ve işleme için stoQ'a gönderilebilir. Suricata veya Bro'dan dosya ayıklamanın işlemiyle birlikte stoQ'un bu dosyaları işlemesi için ayarlanabilmektedir. Tüm yürütülebilir dosyaları, PDF'leri veya Office Belgelerini gönderebilir daha yüksek riskli dosya türlerini otomatik olarak analiz etmeyi sağlar.



Bu konuyla ilgili blog yazısı: <https://medium.com/stoq/using-stoq-with-suricatas-file-extraction-capability-2d2ccc5b3077>

Zenginleştirme

XOR encoded içeriği otomatik olarak işleme özelliği veya base64 decode etmek için dekode eklentileri bulundurur. Arşivleri açma ve PDF belgelerini sadeleştirme gibi görevleri otomatikleştirebilir. Carver eklentileri, Word Belgeleri'nde gömülü olan shell kodu veya flash dosyaları gibi gizli yükleri ayıklamak için kullanılır. Bu zenginleştirilmiş nesneler daha sonra ek işleme için stoQ frameworküne geri gönderilir.

İşleme

Bu süreç, stoQ'nun betiklerle (exiftool, TRiD, Yara, vb.) Ve API'lerle (FireEye, VirusTotal, ThreatCrowd, vb.) Etkileşime girmesine ve nesnelerimizle ilgili daha fazla veri almasına izin verir.

Export

StoQ bir nesneyi alıp, zenginleştirdikten ve işledikten sonra, sonuçlar depolama için bir Bağlayıcı (connector) eklentisine gönderilir. Bu, normal bir metin dosyası veya veritabanı kadar basit veya birden fazla veri merkezine yayılmış birden fazla veritabanı gibi karmaşık bir yapı olabilir.

Bu verileri ElasticSearch veya Splunk gibi bir şeyle kullanmak, stoQ'dan geçen nesneler için bize çok zengin bir meta veri kaynağı sağlayabilmektedir. Büyük ve ayrıntılı veri kümesi, çevrenizdeki daha büyük eğilimleri ve anomalileri bulmak için kullanılabilir. stoQ, bu meta verilerin tümü için sorguları ve uyarıları düzenlemenizi sağlar.

Artık kuruluşunuzdaki tüm yara isabetlerini arayabilir veya işlenmiş tüm dosya adlarını listeleyebilirsiniz.

Web: <https://stoq.punchcyber.com/>

Github: <https://github.com/PUNCH-Cyber/stoq>

Blog: <https://medium.com/stoq>

TekDefense - Automater

Automater URL / Domain, IP Address ve Md5 Hash OSINT (open source threat intelligence) aracıdır ve analiz sürecini saldırı analistleri için kolaylaştırmaktadır.

Bir hedef (URL, IP veya HASH) veya hedeflerle dolu bir dosya verildiğinde Automater, aşağıdaki gibi kaynaklardan ilgili sonuçları döndürecektir. IPvoid.com, Robtex.com, Fortiguard.com, unshorten.me, Urlvoid.com, Labs. alienvault.com, ThreatExpert, VxVault ve VirusTotal...

Kullanımı:

Yüklendikten sonra, Windows, Linux ve Kali genelinde kullanım hemen hemen aynıdır.

```
python Automater.py -h  
veya chmod + x Automater.py ise
```

Örnek kullanım:

```
Python Automater.py <target>  
python Automater.py 37.221.161.215  
  
[*] Checking https://robtex.com/37.221.161.215  
[*] Checking http://www.fortiguard.com/ip_rep/index.php?data=37.221.161.215&lookup=Lookup  
[*] Checking http://www.alienvault.com/apps/rep_monitor/ip/37.221.161.215  
[*] Checking https://www.virustotal.com/en/ip-address/37.221.161.215/information/  
[*] Checking http://www.ipvoid.com/scan/37.221.161.215  
  
_____ Results found for: 37.221.161.215 _____  
  
[+] A records from Robtex.com: vm1033.gigaservers.net  
[+] Fortinet URL Category: Unclassified  
[+] Found in AlienVault reputation DB: http://www.alienvault.com/apps/rep_monitor/ip/37.221.161.215  
  
No results found for: [+] pDNS data from VirusTotal:  
  
[+] pDNS malicious URLs from VirusTotal: ('2013-12-03', 'http://37.221.161(.)215/')  
[+] pDNS malicious URLs from VirusTotal: ('2013-11-30', 'http://37.221.161(.)215/')  
[+] pDNS malicious URLs from VirusTotal: ('2013-11-29', 'http://37.221.161(.)215/cripted.exe%5B/')  
  
No results found for: [+] Blacklist from IPVoid:  
  
[+] ISP from IPvoid: Voxility S.R.L.  
[+] Country from IPVoid: (RO) Romania
```

Forager



"Tüm tehdit istihbaratı verilerini almak, saklamak ve düzenlemek için daha kolay bir yol olup olmadığını hiç merak ettiniz mi? Tüm tehdit istihbarat uygulamalarının "trilyonlarca veri noktasını korele eden" bir veritabanı gerektirmediğini ve bunun yerine basit TXT dosyaları ile, diğer yayınlardan, PDF tehdit raporlarından veya diğer verilerden tehdit verilerini çekebilen basit bir araca ihtiyacınız varsa. Önceden yapılandırılmış 15 tehdit beslemesiyle Forager açık kaynak bir çözüm oluşturuyor."

Özellikler:

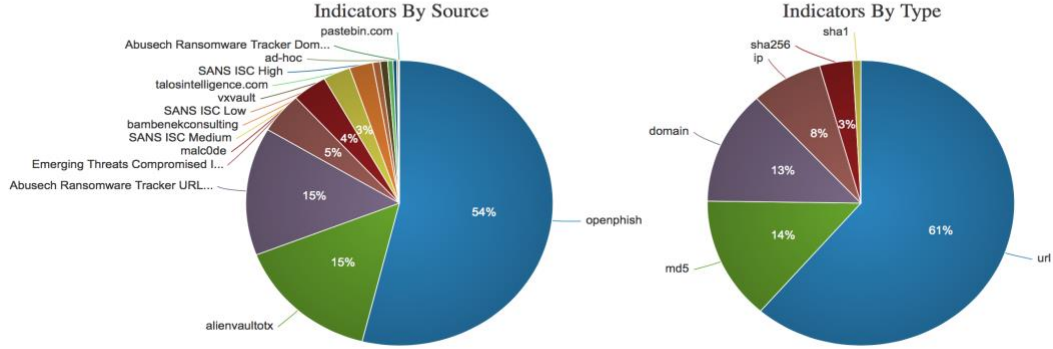
- Modüler feed fonksiyonlarını kullanarak URL'lerden tehdit verilerini alma
- Domain, md5, sha1, sha256, IPv4 ve YARA göstergelerini ayıklama
- Mevcut intel setini tek bir IP ile veya bir IOC dosyasıyla arama
- CarbonBlack tarafından kullanılması için JSON feed'leri üretme
- CarbonBlack için Basit HTTP JSON besleme sunucusu sağlama

Github: <https://github.com/opensourcesec/Forager#summary>

GOSINT Framework

Indicator Metrics

View a breakdown of the indicators currently loaded into GOSINT below.



Yazımızda da bahsettiğimiz gibi internet üzerinde halihazırda çok fazla açık kaynak tehdit istihbarat aracı bulunmaktadır. Ancak bu konu hakkında yararlı bilgi bulmak, toplamak ve filtrelemek için kolay bir yol bulunmamaktadır. GOSINT, bir güvenlik analistinin yapılandırılmamış tehdit istihbaratını toplamasına ve standartlaştırmasına olanak tanımaktadır.

GOSINT'i tehdit göstergeleri için bir transfer istasyonu olarak düşünebilirsiniz. Yazılım, tehdit istihbaratı analistlerine bir göstergenin izleme değerinde olup olmadığını veya reddedilmesi gerektiğini değerlendirmesine izin verir. Bu karar verme aşaması, herhangi bir tehdit göstergesini yönetmede çok önemlidir. Hem bir insan analisti hem de GOSINT'in kendisi tarafından tetkik edilmesi, göstergelerin tehdit algılama etkinliğini artırır. Ekleyebileceğiniz gösterge kaynakları sayısında da bir sınır bulunmamaktadır.

Github: <https://github.com/ciscocsirt/gosint>

Loki IOC Scanner

```
LOKI
IOC Scanner

(C) Florian Roth
December 2016
Version 0.18.0

DISCLAIMER - USE AT YOUR OWN RISK

[NOTICE] Starting Loki Scan SYSTEM: PROMETHEUS TIME: 20161210T00:14:37Z PLATFORM: windows
[INFO] File Name Characteristics initialized with 1640 regex patterns
[INFO] C2 server indicators initialized with 19817 elements
[INFO] Malicious MD5 Hashes initialized with 11753 hashes
[INFO] Malicious SHA1 Hashes initialized with 4311 hashes
[INFO] Malicious SHA256 Hashes initialized with 11865 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder X:\Workspace\Loki\signature-base\yara
[INFO] Initializing Yara rule apt_allenspy_rat.yar
[INFO] Initializing Yara rule apt_apt17_malware.yar
[INFO] Initializing Yara rule apt_apt28.yar
[INFO] Initializing Yara rule apt_apt30_backspace.yar
[INFO] Initializing Yara rule apt_apt6_malware.yar
[INFO] Initializing Yara rule apt_backdoor_ssh_python.yar
[INFO] Initializing Yara rule apt_backspace.yar
```

LOKI, APT Tarayıcısı THOR'un ana analiz modüllerinin tam bir yeniden yazımı olan ücretsiz ve basit bir IOC (tehdit göstergeleri) tarayıcısıdır. Bu tehdit göstergeleri, labınızda oluşturduğunuz olay raporlarından, adli bilişim analizlerinden veya zararlı yazılım örneklerinden elde edilebilir. LOKI, sistemlerinizi bilinen IOC'ler için taramanın basit bir yolunu sunmaktadır.

- MD5 / SHA1 / SHA256 hashleri
- Yara Kuralları
- Regex(Düzenli ifadeler) (ör. \\testdirectory\\.exe)
- Dosya isimleri ve dizinler

```
[WARNING]
FILE: C:\testing\appdata\mozilla\dre.bin SCORE: 80 TYPE: EXE SIZE: 66252
FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ
MD5: d6278a53daea5f16e7d2fbec40d5438e
SHA1: 02df5a727b4b9299037600c17d8444244ab0d249
SHA256: 4d54bec2da63ad3535e51c508db075025539349d79506073562f79ce127b163f CREATED: Mon Feb 16 19:20:09 2015 M
ODIFIED: Mon Nov 10 23:56:57 2014 ACCESSED: Mon Feb 16 19:20:09 2015
REASON_1: File Name IOC matched PATTERN: (application data|AppData|Anwendungsdaten)\\mozilla\\[~\\]+\\.bin SU
BSCORE: 80 DESC: Kaspersky Carbanak APT Malware Hash http://goo.gl/0Nhx2
[NOTICE]
FILE: C:\testing\excludes\temp.edb SCORE: 50 TYPE: EXE SIZE: 657392
FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ
MD5: d8b7b276710127d233abcb7313aac36
SHA1: 27011d2fc22e894bd8a48de03a82b64f0bdbbabc
SHA256: 55a1612963fed3094e0c6817112dbdde5b2d24c2bc0d76e8435d0a5b108b9e57 CREATED: Sat Apr 18 12:51:19 2015 M
ODIFIED: Fri Jul 06 09:59:22 2012 ACCESSED: Sat Apr 18 12:51:19 2015
REASON_1: Yara Rule MATCH: HackTool Producers SUBSCORE: 50
DESCRIPTION: Hacktool Producers String
MATCHES: Str1: gentilkiwi.com
[ALERT]
FILE: C:\testing\excludes\Exchange Server\ClientAccess\0AB\its_mimi.exe SCORE: 160 TYPE: EXE SIZE: 418304
FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ
MD5: 1cb84e9e7855738207e25bd4b2b400bd
SHA1: cf89deb5fcb58930d73cdab18651ceabb8285bf6
SHA256: 3a04c554f8a5458a86bfd5e84ca5e4495e109dfaf857333677d899b15d722a70 CREATED: Thu Mar 24 10:57:55 2016 M
ODIFIED: Sun Jan 31 16:02:26 2016 ACCESSED: Thu Mar 24 10:57:55 2016
REASON_1: Yara Rule MATCH: Powerkatz_DLL_Generic SUBSCORE: 80
DESCRIPTION: Detects Powerkatz - a Mimikatz version prepared to run in memory via Powershell (overlap with o
ther Mimikatz versions is possible)
MATCHES: Str1: kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM Accounts (0x%08x) Str2: k
uhl_m_lsadump_getComputerAndSyskey ; kuh ... (truncated)
REASON_2: Yara Rule MATCH: mimikatz SUBSCORE: 80
DESCRIPTION: mimikatz
MATCHES: Str1: L\x03\u00fffdI\u00fffd\x03H\u00fffd Str2: L\u00fffdI\u00fffd\u00fffd\u00fffd\u00fffdL\u003\u00fffd
```

Github: <https://github.com/Neo23x0/Loki>

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "*Siber Güvenlik Kampları*", "*Siber Güvenlik Staj Okulu*", "*Siber Güvenlik Ar-Ge Destek Bursu*", "*Ethical Hacking yarışmaları*" ve "*Siber Güvenlik Kütüphanesi*" gibi birçok gönüllü faaliyetin destekleyici olmuştur.