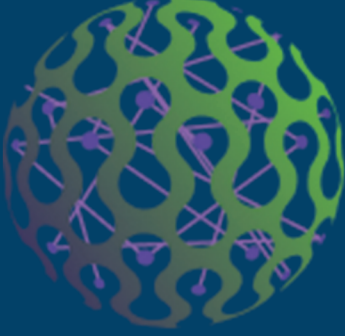




INTER
PROBE
INTELLIGENCE & ANALYTICS

Zararlı Yazılım Trendleri

Hazırlayan
INTERPROBE

İçindekiler

01 InterProbe Hakkında

InterProbe ve Hizmetleri 03

Giriş / Yönetici Özeti

Giriş 04

Yönetici Özeti 05

03 Zararlı Yazılım Trendleri

CloudMensis 06

Autolycos 08

ChromeLoader 10

MedusaLocker 12

Lilith Ransomware 14

04 Kaynakça

05 Bize Ulaşın

INTELLIGENCE ANALYTICS

InterProbe



Temmuz 2022 - Zararlı Yazılım Trendleri

InterProbe Hakkında

InterProbe



InterProbe, özellikle hassas faaliyet alanlarında çalışan kuruluşlarla beraber her sektörden kuruluşların değişen teknolojik ihtiyaçlarını karşılamak için benzersiz ürünler, çözümler ve hizmetler tasarlar. Yüksek nitelikli mühendisler ve uzmanlardan oluşan ekibimiz ile yeni nesil teknolojileri tasarlamakta ve üretmekteyiz. Geliştirdiğimiz yazılımlarımız ile işinize değer katmak için çalışan gerçek bir ortağız.

Ankara'daki merkez ofisimiz, İstanbul Teknopark şubemiz ve yurt dışında Azerbaycan, Katar ve Kazakistan'daki ofislerimiz ile dünyadaki tüm kuruluşlara stratejik çözümler sunmaktayız. Ar-Ge yatırımlarımız ve güvenlik teknolojilerindeki trendleri yakından takip etmemizden dolayı uluslararası çaptaki kuruluşlarla iş birliği yapmaktayız. Türkiye'nin kalkınması ve büyümesi için güçlü bir sorumluluk duygusuna sahibiz; bu duygu, çalışmalarımıza yön veren en güçlü arzudur. InterProbe, özellikle genç mezunların ve üniversite öğrencilerinin yetkinlik ve becerilerini geliştirmeye yönelik eğitim ve staj programları düzenlemektedir. Ayrıca genç yazılımcılara proje desteği vermek için kaynak ayırmaktayız.

Birçok başarılı projeye imza atan Pavo Grup şirketlerinin bir parçası olarak ulusal kaynak ve yeteneklerle geliştirilmiş uçtan uca çözümleri bünyemizde sunmaktayız:

Savunma sanayiinde uzun yıllardır faaliyet gösteren ve ağırlıklı olarak dijital iletişim ve gömülü yazılım alanlarında hizmet veren **PAVOTEK**,

Elektromekanik üretim, montaj (SMD,THT) ve test konusunda uzmanlaşmış olan **PANOD**,

Aviyonik sistemler, askeri elektronik ve iletişim sistemleri, biyomedikal çözümler, güç elektroniği ve IoT alanlarında faaliyet gösteren **PAVELSIS**,

Ağ güvenliği ürünleri ve anahtarlama yönlendirme cihazları tasarlayan ve üreten **PNETWORKS**, Veri merkezleri için inşaat, altyapı ve kurulum hizmetleri sunan InterData olmak üzere geleceğe emin adımlarla ilerlemekteyiz.

Siber güvenlik her geçen gün daha fazla önem kazanmakta. Artık bir sistemi ele geçirmek ya da o sistemi saldırganlardan korumak çok daha zor. 2000'li yıllarda basit telnet zafiyeti ile ele geçirilebilen sistemler, standartlaşmış kütüphanelerin kullanımının yaygınlaşması ve siber güvenlik bilincinin artması gibi sebeplerden dolayı artık eskisi kadar yaygın değil. Bu nedenle saldırganlar da yeni stratejiler edindiler. Artık güvenliğin en zayıf halkalarından birinin insan olduğu daha fazla göze çarptı ve ortalama saldırılarının etkinliğinin arttığı görüldü. Saldırganlar bunun yanında yeni bir zafiyet bulunduğunda güncellenmesi zaman alacak sistemlerinde peşinde koşar oldular. Tabi her ne kadar bu teknikler etkili olsa da saldırganlar bununla beraber tekniklerini farklı yollarla değiştirmek durumundalar aksi takdirde imza tabanlı tarama sistemleri tarafından hızlıca tespit edilirler. Bu nedenle saldırganlar gönderdikleri zararlı kodları değiştirmenin hızlı yollarını geliştirdiler. İmza tabanlı sistemler bu tehditleri tespit etmekte yetersiz olduğundan hamle yapma sırasının onlara geldiğini anlayan siber güvenlik ekipleri zararlı yazılımların davranışlarını takip etmenin daha etkili olduğunu fark ettiler.

Bu noktada siber güvenlik ekiplerinin mevcut trendleri takip etmesini kolaylaştırmak adına InterProbe Fusion Center ekibi olarak InterProbe Zararlı Yazılım Bülteni'nin ikinci sayısı ile karşınızdayız. Bültenimiz teknik detaylar ile fazla meşgul olmayan ve siber güvenliğe dair ilgisi olan hemen herkesin anlayabileceği bir dilde, trend olan zararlı yazılımları, zararlıyı kullanan tehdit aktörlerinin mevcut aktiviteleri ve kullandıkları yeni teknikleri bulunduracak şekilde aylık olarak yayınlanacak.

Keyifli okumalar.

Yönetici Özeti

InterProbe

Siber güvenlik evreni her zamanki gibi yine hareketli geçiyor. Bu ay sizler için derlediğimiz araştırmalarımız:

-  ESET araştırmacıları MacOS kullanıcılarını tehdit eden yeni bir zararlı yazılım türü olduğunu açıkladı. CloudMensis adı verilen bu zararlı yazılım MacOS kullanıcılarının kişisel verilerinin peşinde.
-  Zararlı yazılımlar aynı zamanda Google Play Store üzerinden de yayılabiliyor. Autolycos adında bir zararlı yazılımın 3 milyon defa indirildiği ortaya çıktı.
-  Zararlı yazılımlar artık daha farklı yayılma teknikleri kullanmaya başlıyor. ChromeLoader zararlı yazılımı QR kodları üzerinden kullanıcıları tehdit ediyor.
-  MedusaLocker fidye yazılımı sağlık dünyasını tehdit etmeye devam ediyor. FBI bu zararlı yazılımın yeniden hareketlendiğini bildirdi.
-  Fidye yazılımları ailesine yeni bir üye daha katıldı. Lilith fidye yazılımının Babuk fidye yazılımı ile benzer kodlara sahip olduğu iddia ediliyor.

CloudMensis

InterProbe

ESET arařtırmacıları son g nlerde kullanıcıları tehdit eden yeni bir zararlı yazılım t r  olduėunu a ıkladı. "CloudMensis" adı verilen bu zararlı yazılım MacOS, iOS, iPadOS cihazlarını hedef alan bir casus yazılım olarak nitelendirilmiřtir. CloudMensis zararlı yazılımı "Objective-C" programlama dili ile geliřtirilmiřtir. Zararlı yazılım analistleri bu tehdidin kullanıcılara nasıl bulařtıėını daha    emediklerini fakat kod y r tme ve yetki y kseltme iřlemlerinin hangi ařamada olduėunu bulduklarını s ylemektedir.

CloudMensis yazılımı MacOS sisteminde bulunan ve kullanıcıların app store' dan yazılım indirme iřlemlerinde izin kontrollerini saėlayan "Transparency Consent and Control (TCC)" adlı bir g venlik sistemini atlattıėı g r lm řt r. TCC kuralları sistem b t nl ė  g venliėi "System Integrity Protection (SIP)" adı verilen bir g venlik mekanizması ile korunmaktadır. Eėer SIP mekanizması aktif deėilse zararlı yazılım izinleri kendisi aktif edebilmektedir. Bazı sistemlerde SIP mekanizması aktif ama o sistemlerin s r mleri "Catalina 10.15.6" s r m nden eskiyse CloudMensis "CVE-2020-9943" kodlu g venlik a ıėını s m rerek etkinliėini s rd rebilmektedir.

Eset arařtırmacılarının yorumlarına g re zararlı yazılıma ait olan kodun kalitesi ve kullanılan obfuscation y ntemleri baz alındıėında tehdit akt rlerinin MacOS yazılımı geliřtirme bilgisinin biraz zayıf olduėunu belirtmiřtir.



"We still do not know how CloudMensis is initially distributed and who the targets are. The general quality of the code and lack of obfuscation shows the authors may not be very familiar with Mac development and are not so advanced. Nonetheless, a lot of resources were put into making CloudMensis a powerful spying tool and a menace to potential targets."

CloudMensis zararlı yazılımı kod yürütme ile sistem üzerinde gerekli yetkileri elde ettiği anda Dropbox, pCloud veya Yandex gibi bulut sunuculardan kendisine ait olan bir casus ajanı indirir. İndirilen bu casus ajanı ilk çalışan zararlı yazılımın aksine daha donanımlıdır. Ve son olarak artık casus ajanı çeşitli bulut sunucuları ile birer erişim anahtarı kullanarak haberleşerek veri kaçırma faaliyetlerine başlar.



CloudMensis MITRE ATT&CK Matrix

InterProbe

Persistence	T1543.004	Create or Modify System Process: Launch Daemon	The CloudMensis downloader installs the second stage as a system-wide daemon.
Defense Evasion	T1553	Subvert Trust Controls	CloudMensis tries to bypass TCC if possible.
Collection	T1560.002	Archive Collected Data: Archive via Library	Archive Collected Data: Archive via Library CloudMensis uses SSZipArchive to create a password-protected ZIP archive of data to exfiltrate.
	T1056.001	Input Capture: Keylogging	CloudMensis can capture and exfiltrate keystrokes.
	T1113	Screen Capture	CloudMensis can take screen captures and exfiltrate them.
	T1005	Data from Local System	CloudMensis looks for files with specific extensions.
	T1025	Data from Removable Media	CloudMensis can search removable media for interesting files upon their connection.
	T1114.001	Email Collection: Local Email Collection	CloudMensis searches for interesting email messages and attachments from Mail.
Command and Control	T1573.002	Encrypted Channel: Asymmetric Cryptography	The CloudMensis initial report is encrypted with a public RSA-2048 key.
	T1573.001	Encrypted Channel: Symmetric Cryptography	CloudMensis encrypts exfiltrated files using password-protected ZIP archives.
	T1102.002	Web Service: Bidirectional Communication	CloudMensis uses Dropbox, pCloud, or Yandex Drive for C&C communication.
Exfiltration	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	CloudMensis exfiltrates files to Dropbox, pCloud, or Yandex Drive.

Önlemler ve İyileştirmeler

- Bilinmeyen kaynaklardan gelen E-Mail eklerini açmamak.
- Sadece "App Store" gibi güvenilir kaynaklardan yazılımlar yüklemek.
- MacOS cihazlarında "System Integrity Protection (SIP)" güvenlik mekanizması aktif durumda olmalıdır

Özellikler

InterProbe

01

Saldırganların dosya indirmelerine olanak sağlamak.

02

Kullanıcıların klavye girdilerini ele geçirmek.

03

Enfekte olan cihazların ekran görüntülerini almak.

04

E-Mail içerikleri, dokümanlar, harici bellekte bulunan dosyalar gibi çeşitli hassas verileri kaçırmak.

05

pCloud, Yandex Disk, Dropbox gibi Cloud servisleri ile haberleşerek komut alma, veri indirme ve veri kaçıрма.

06

Herhangi bir exploit kullanmadan MacOS sisteminin savunma mekanizmalarını atlatmak.

07

Sistemde çalışan prosesleri listeleme.



Autolycos

Evina kuruluşunda çalışan güvenlik araştırmacılarından Maxime Ingaro 2021 yılının Haziran ayında Google Play Store platformunda gizlenmiş olan bir zararlı yazılımı tespit etti. Tespit edilen bu zararlı yazılım "SpyJoker" adlı zararlı yazılımın yeni bir varyantıydı. Ingaro bu zararlı yazılıma "Autolycos" adını verdi ve daha sonra tespit etmiş olduğu bulguları Google' a açıkladı ama Google bulguların açıklanmasından ancak 6 ay sonra zararlı olarak bildirilen 8 uygulamanın sadece 6 tanesini tespit edebilmiş ve bu uygulamaları da Play Store' dan kaldırmıştır.

13 Temmuz günü Maxime Ingaro 8 zararlı uygulamadan geriye kalan diğer 2 zararlı uygulamanın hala Play Store üzerinden indirildiğini bildirmiştir. Google bu kez yapılan bildirimlere hızlı aksiyon almış ve kalan 2 uygulamayı da Play Store' dan kaldırmıştır. İşin korkutucu tarafı ise bu uygulamalar 3 milyondan fazla indirilme almış ve hala başka kullanıcıların cihazlarında bu zararlı yazılımlar barındırılıyor olabilir.

Autolycos

InterProbe

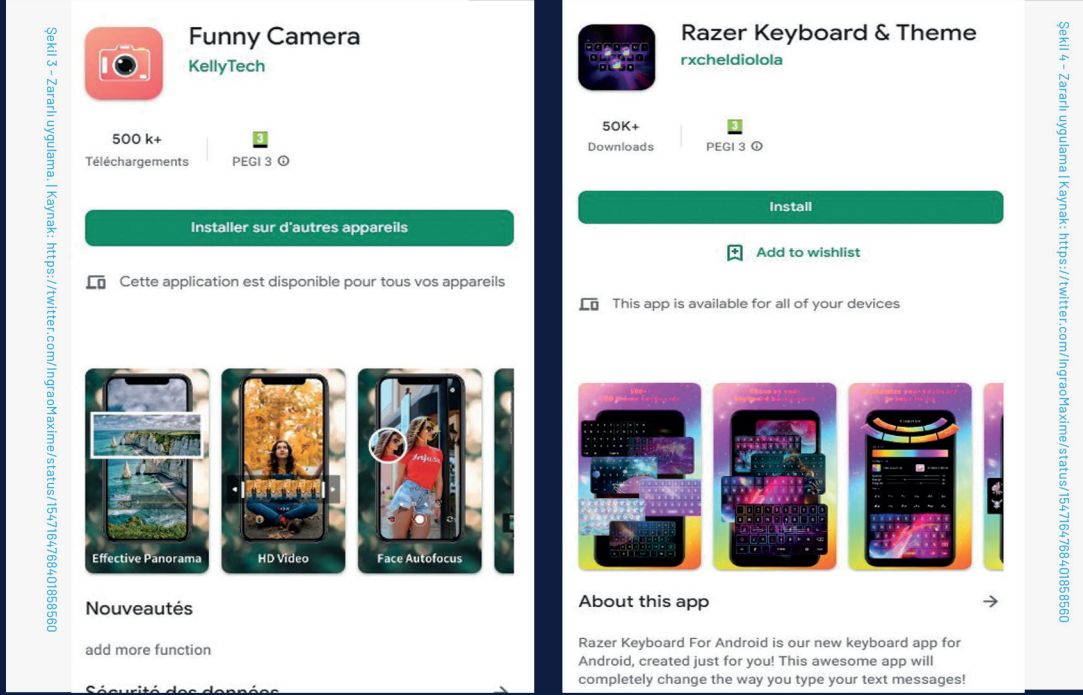
Eğer cihazınızda aşağıda belirttiğimiz uygulamalar yüklü ise bir an önce cihazınızdan bu uygulamaları kaldırmanız gerekmektedir.

Bu uygulamalar:

- Vlog Star Video Editor (com.vlog.star.video.editor): **1 milyon indirilme**
- Creative 3D Launcher (app.launcher.creative3d): **1 milyon indirilme**
- Wow Beauty Camera (com.wowbeauty.camera): **100.000 indirilme**
- Gif Emoji Keyboard (com.gif.emoji.keyboard): **100.000 indirilme**
- Razer Keyboard & Theme (com.razer.keyboards): **10.000 indirilme**
- Freeglow Camera 1.0.0 (com.glow.camera.open): **5.000 indirilme**
- Coco Camera v1.1 (com.toomore.cool.camera): **1.000 indirilme**

Autolycos

InterProbe



Özellikleri

- ✓ SMS içeriklerine erişim
- ✓ OTP verilerine erişim
- ✓ Webview kullanmak yerine uzak tarayıcı üzerinden HTTP istekleri yapıp premium servislere kaydolmak.

Autolycos MITRE ATT&CK Matrix

Hash: 95547426cd892cc50547d65aef7edb82212c68a44257318cb89bfafa04889bb

MITRE ATT&CK™ Techniques Detection

InterProbe

Execution						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1402	Broadcast Receivers	- Persistence - Execution	An intent is a message passed between Android application or system components. Learn more	1 confidential indicators		
Persistence						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1402	Broadcast Receivers	- Persistence - Execution	An intent is a message passed between Android application or system components. Learn more	1 confidential indicators		
Defense Evasion						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1418	Application Discovery	- Defense Evasion - Discovery	Adversaries may seek to identify all applications installed on the device. Learn more		1 confidential indicators	
Discovery						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1418	Application Discovery	- Defense Evasion - Discovery	Adversaries may seek to identify all applications installed on the device. Learn more		1 confidential indicators	
T1421	System Network Connections Discovery	Discovery	On Android, applications can use standard APIs to gather a list of network connections to and from the device. Learn more			Tests the internet connectivity
Collection						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1114	Email Collection	Collection	Adversaries may target user email to collect sensitive information. Learn more		Found a potential E-Mail address in binary/memory	
T1429	Capture Audio	Collection	Adversaries may capture audio to collect information on a user of a mobile device using standard operating system APIs. Learn more		Has the ability to record audio	
Command and Control						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1573	Encrypted Channel	Command and Control	Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Learn more			Possibly tries to communicate over SSL connection (HTTPS)
Impact						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1486	Data Encrypted for Impact	Impact	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. Learn more		Found a cryptographic related string	

Önlemler ve İyileştirmeler

- Google Play Store vb. platformlardan uygulamalar indirirken indirilen uygulamaların istemiş oldukları izinler kontrol edilmelidir.
- Google Play Store' dan uygulama kurmadan önce uygulama ile ilgili yapılmış olan yorumlar gözden geçirilmelidir.
- Facebook vb. sosyal medya ortamlarında bulunan reklamlara dikkat edilmeli ve reklamlar aracılığı ile indirilen uygulamalara güvenilmemelidir.

ChromeLoader

InterProbe

Siber güvenlik arařtırmacıları Temmuz ayında "ChromeLoader" bir dięer adıyla "Choziosi Loader" zararlısına ait yeni varyantların olduęunu bildirdiler. ChromeLoader Ocak 2022 tarihinde ortaya çıkan ve Windows ve MacOS kullanıcılarının cihazlarında bulunan Chrome uygulamasına zararlı eklentiler kurup tarayıcılarını ele geçiren bir zararlı yazılımdır. Dięer zararlı yazılımlara nazaran daha farklı bir bulařma yöntemi kullanmaktadır. Bu yöntem QR kodları aracılığıyla korsan içerikleri paylaşan tweetlerdir. Kullanıcılar bu tweetlerdeki QR kodlarını okuttukları zaman cihazlarına birer ISO, DMG veya AHK dosyası indirilmektedir. Bu dosyalarda bulunan içerikler zararlı yazılım tarafından "PowerShell" yardımı ile kurularak kullanıcıya ait olan tarayıcıyı enfekte etmiş olur. RedCanary' deki arařtırmacılar bu yöntemin çok sık görölmedięini ve güvenlik cihazları tarafından sıklıkla tespit edilmedięini belirtmiştir.

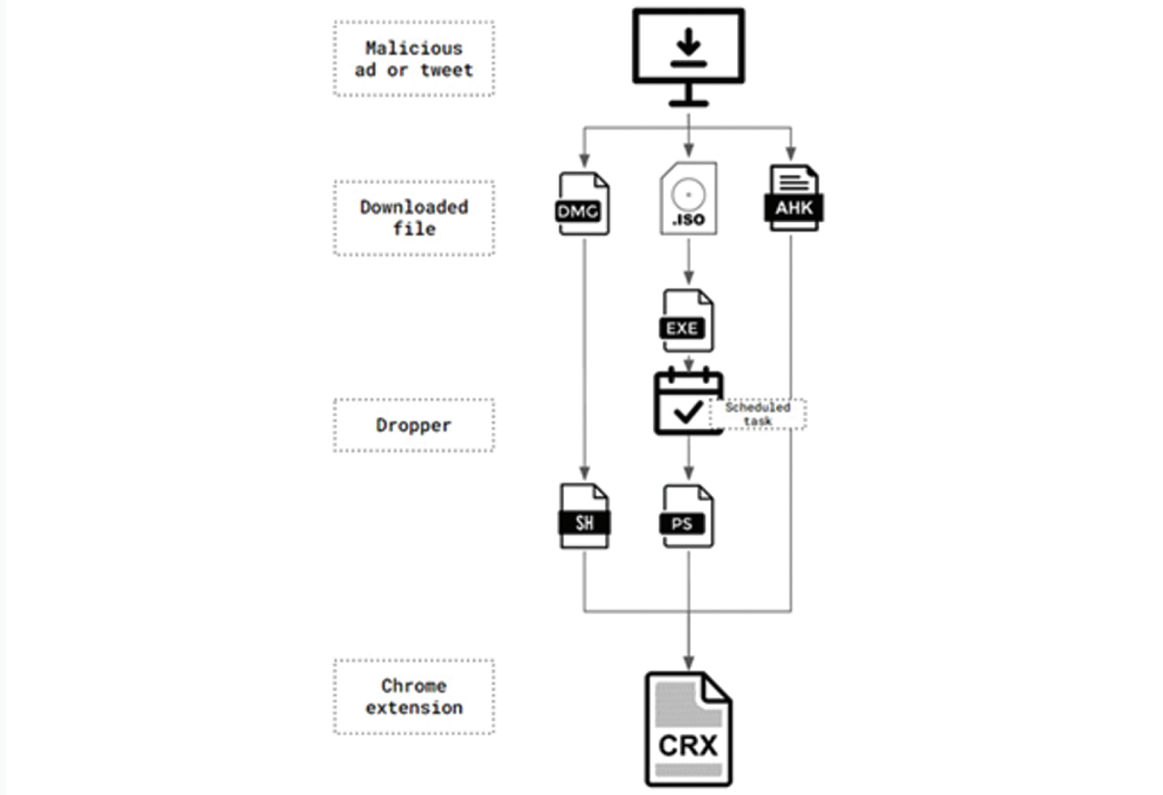
Tarayıcıya kurulan zararlı eklenti artık kullanıcıları reklamcılık sitelerine yönlendirerek zararlı yazılımların bulařması, veri ihlali ve kimlik hırsızlıęı gibi çeřitli sorunların gerekleşmesine neden olacaktır.

İlerleyen zamanlarda Colin Cowie adında bir siber güvenlik arařtırmacısı MacOS variantının analiz raporunu yayınlamıştır. MacOS variantı Chrome ve Safari uygulamalarını enfekte etmektedir. Kullanılan enfeksiyon teknięi Windows varyantında olduęu gibi betik dillerinin (powershell, bash, sh) kullanımıyla gerekleşmektedir.



ChromeLoader

InterProbe



Şekil 5 - ChromeLoader çalışma aşamaları | Kaynak: <https://unit42.paloaltonetworks.com/chromeloader-malware/>

Özellikleri

01

Obfuscation ve kullanılan teknikler ile güvenlik cihazlarını atlatmak.

02

Tarayıcı verilerini okumak ve manipüle etmek.

03

Kullanıcıları reklamcılık sitelerine yönlendirmek.

ChromeLoader MITRE ATT&CK Matrix

InterProbe

Defense Evasion						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1027.002	Software Packing	Defense Evasion	Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more			- Matched Compiler/Packer signature 61d8...c9c1
Credential Access						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	- Credential Access - Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more		- Installs hooks/patches the running process 61d8...c9c1	
Discovery						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1120	Peripheral Device Discovery	Discovery	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Learn more			- Queries volume information 61d8...c9c1
T1082	System Information Discovery	Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more		- Reads the cryptographic machine GUID 61d8...c9c1	- Contains ability to read software policies 61d8...c9c1
T1012	Query Registry	Discovery	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more		- Reads information about supported languages 61d8...c9c1 - Reads the active computer name 61d8...c9c1	
Collection						
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	- Credential Access - Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more		- Installs hooks/patches the running process 61d8...c9c1	

Önlemler ve İyileştirmeler

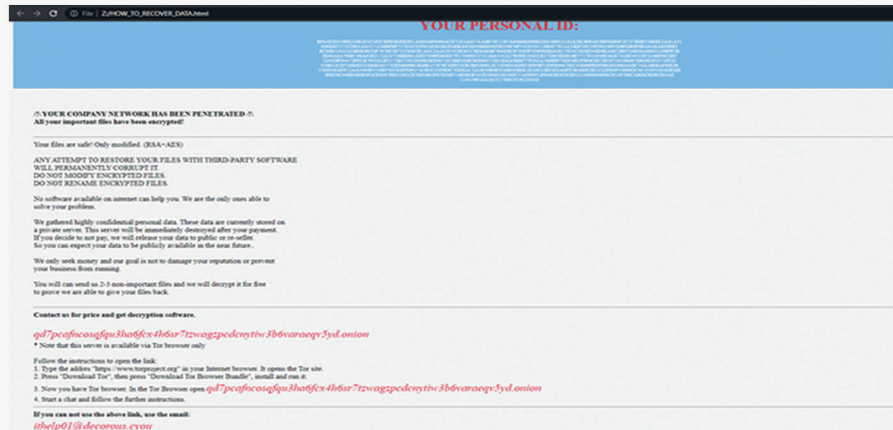
- Yalnızca güvenilir kaynaklardan eklentiler kurmak.
- Korsan yazılım barındıran platformlardan uzak durmak.
- E-Mail eklerine ve mesajlara dikkat etmek.
- Güvenlik yazılımlarının aktif ve güncel olduğundan emin olmak.
- Sistem üzerinde çalışan powershell/bash prosesleri kontrol edilmeli eğer base64 ile encode edilmiş parametreler varsa sistem üzerinde inceleme yapılması gerekmektedir.

MedusaLocker Ransomware

InterProbe

FBI(Federal Bureau of Investigation), CISA(Cybersecurity and Infrastructure Security Agency) ve FinCEN, 2019 yılında ransomware pazarına atılan MedusaLocker zararlısının 2022 Mayıs ayı civarında tekrardan hareketlendiğini bildirdi. Sağlık sektörünü hedef alan MedusaLocker, Covid-19 salgınına fırsata çeviren zararlılardan biridir. .

Zararlının, zararlıyı geliştiren yazılımcının zararlıyı dağıtan ortaklar ile beraber çalıştığı RaaS (Ransomware as a Service) modelini izlediği düşünülüyor. Fidyelerin %55-60'ının bir hesaba kalanın ise farklı bir hesaba aktarılıyor olması da bu modelin kullanıldığını destekler nitelikte.



Şekil 6 - Fidye Bilgilendirme Metni, iletişim için bırakılan e-posta ve .onion domainleri de bu dosyada bulunmakta.

Zararlı, şifrelediği dosyaların bulunduğu her klasöre bir bilgilendirme metni bırakmaktadır. Şifrelenen dosyaların uzantısı farklı varyasyonlarda değişiklik göstermektedir.

beautify.js.marlock011	7/25/2022 7:02 AM	MARLOCK011 File	41 KB
hexed.ocx.marlock011	7/25/2022 7:02 AM	MARLOCK011 File	377 KB
HOW_TO_RECOVER_DATA.html	7/25/2022 7:02 AM	Microsoft Edge H...	5 KB
iTextFilters.dll	12/14/2016 3:50 AM	Application exten...	25 KB
iTextFilters.tlb.marlock011	7/25/2022 7:02 AM	MARLOCK011 File	9 KB
iTextSharp.dll	12/14/2016 3:50 AM	Application exten...	3,348 KB
java.hiligher.marlock011	7/25/2022 7:02 AM	MARLOCK011 File	9 KB
js_api.txt.marlock011	7/25/2022 7:02 AM	MARLOCK011 File	9 KB
JS_UI_Readme.txt.marlock011	7/25/2022 7:02 AM	MARLOCK011 File	9 KB

Şekil 7 - Şifrelenmiş dosyalar ve fidye bilgilendirme metni dosyası. Bu varyant için şifrelenmiş dosyaların uzantısı ".marlock011" şeklinde.

Tehdit aktörleri genellikle e-posta üzerinden ortalama saldırıları ve hatalı konfigüre edilmiş RDP (Remote Desktop Protocol) servislerine yapılan saldırılar ile sistemlere erişim sağlamaktadırlar.

MedusaLocker Ransomware

MITRE ATT&CK Matrix

InterProbe

Execution

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1047	Windows Management Instrumentation	Execution	Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. Learn more		- Contains references to WMI/WMIC 6250..0812 - Reads system information using Windows Management Instrumentation Commandline (WMIC) 6250..0812	
T1559.001	Component Object Model	Execution	Adversaries may use the Windows Component Object Model (COM) for local code execution. Learn more	1 confidential indicators		

Privilege Escalation

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1055	Process Injection	- Privilege Escalation - Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more	- Writes data to a remote process 6250..0812		
T1548.002	Bypass User Account Control	- Privilege Escalation - Defense Evasion	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Learn more		- References COM interfaces strings prone to UAC bypass 6250..0812	
T1055.012	Process Hollowing	- Privilege Escalation - Defense Evasion	Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Learn more	- Allocates virtual memory in a remote process 6250..0812		

Defense Evasion

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1055	Process Injection	- Privilege Escalation - Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more	- Writes data to a remote process 6250..0812		
T1548.002	Bypass User Account Control	- Privilege Escalation - Defense Evasion	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Learn more		- References COM interfaces strings prone to UAC bypass 6250..0812	
T1055.012	Process Hollowing	- Privilege Escalation - Defense Evasion	Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Learn more	- Allocates virtual memory in a remote process 6250..0812		
T1027.002	Software Packing	Defense Evasion	Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more			- Matched Compiler/Packer signature 6250..0812
T1112	Modify Registry	Defense Evasion	Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Learn more	- Modifies the UAC/LUA settings (Account Control) 6250..0812		
T1497	Virtualization/Sandbox Evasion	- Defense Evasion - Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more		- Possibly tries to implement anti-virtualization techniques 6250..0812	
T1564.004	NTFS File Attributes	Defense Evasion	Adversaries may use NTFS file attributes to hide their malicious data in order to evade detection. Learn more		1 confidential indicators	

MedusaLocker Ransomware

MITRE ATT&CK Matrix

InterProbe

Credential Access

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	- Credential Access - Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more		- Installs hooks/patches the running process 6250..0812	

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1120	Peripheral Device Discovery	Discovery	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Learn more			- Queries volume information 6250..0812
T1012	Query Registry	Discovery	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more		- Reads information about supported languages 6250..0812 3 confidential indicators	
T1057	Process Discovery	Discovery	Adversaries may attempt to get information about running processes on a system. Learn more		- Queries process information 6250..0812	- Observed Process32First/Process32Next/CreateToolhelp32Snapshot API string 6250..0812
T1082	System Information Discovery	Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more		- Reads the cryptographic machine GUID 6250..0812	- Contains ability to read software policies 6250..0812
T1083	File and Directory Discovery	Discovery	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Learn more	- Tries to access unusual system drive letters 6250..0812		
T1497	Virtualization/Sandbox Evasion	- Defense Evasion - Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more		- Possibly tries to implement anti-virtualization techniques 6250..0812	

Collection

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	- Credential Access - Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more		- Installs hooks/patches the running process 6250..0812	
T1114	Email Collection	Collection	Adversaries may target user email to collect sensitive information. Learn more		- Found a potential E-Mail address in binary/memory 6250..0812	

Impact

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1490	Inhibit System Recovery	Impact	Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. Learn more	- Deletes volume snapshots (often used by ransomware) 6250..0812		

Önlemler ve İyileştirmeler

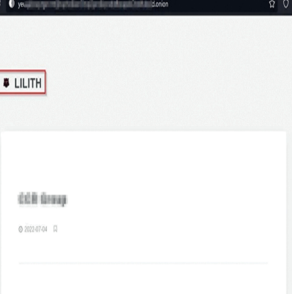
- Önemli verilerinizi düzenli olarak yedekleyin. Yedeklerinizin sisteminizden izole edilmiş olmasına özen gösterin.
- Çalışanlarınızı sosyal mühendislik ve oltalama tekniklerine karşı eğitin.
- Powershell kullanımını sadece imzalı kodları çalıştıracak şekilde konfigüre edin.
- Uzaktan bağlantı servislerini dış ağa açmaktan kaçının. Dış ağdan bağlanılması gereken durumlar için VPN gibi servisler kullanılabilir.
- Çok faktörlü doğrulama kullanın.

InterProbe

 **JAMESWIT**
@JAMESWIT_MHT

#Ransomware #Liith ?
👉👉👉
bazaar.abuse.ch/sample/f3c0a04...

art files have been encrypted and stolen!
price and get decryption software.
to contact us for negotiation.
contact within three days, we'll start leaking data.1) Contact our tor
address: <https://tor.chyt.org/polson.id>
788232555651FC749E953546FC6A0698C7812097D193C706B0A758A282*
server is available via tor browser only
irection to open the link:
pres "<https://www.torproject.org/>" In your Internet browser. It opens
Load Tor", then press "Download Tor Browser Bundle", install and run
tor browser. In the Tor Browser browser:
nytg9mrt1juphs6w5ctmp2z9sr6ndpafaspek3z4d4bcd1.onion



\\Restore_Your_Files.txt	boot.ini
Restore_Your_Files.txt	bootfont.bin
Windows	bootsect.bak
Windows.old	bootmgr
Tor Browser	bootmgr.efi
Internet Explorer	bootmgfw.efi
Google	desktop.ini
Opera	iconcache.db
Opera Software	nltldr
Mozilla	ntuser.dat
Mozilla Firefox	ntuser.dat.log
\$Recycle.Bin	ntuser.ini
ProgramData	thumbs.db
All Users	ecdln_pub_k.bin
autorun.inf	Program Files
	Program Files [x86]

Zararlının dosyaları şifrelerken çalıştırılabilir olan .exe, .sys, .dll dosyalarını atladığı gözlemlendi. Sistemin ve zararlıının çalışması için gerekli olan bazı dosyalarında şifrelenmeden atlandığı görüldü. Cyble araştırmacıları, bu atlama listesinde “ecdh_pub_k.bin” isimli bir dosya olduğunu fark etti. Bu dosyanın ise BABUK Ransomware’ın şifreleme modülünün bir parçası olduğu biliniyor. Bu bulgu Lilith’in BABUK Ransomware’ın kodlarının bir kısmının tekrar kullanılarak geliştirildiğini destekliyor.

Lilith Ransomware

MITRE ATT&CK Matrix

InterProbe

Defense Evasion

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1497	Virtualization/Sandbox Evasion	- Defense Evasion - Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more	- The input sample contains a known anti-VM trick 62c3...3589		
T1027.002	Software Packing	Defense Evasion	Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more		1 confidential indicators	
T1070.004	File Deletion	Defense Evasion	Adversaries may delete files left behind by the actions of their intrusion activity. Learn more		- Opens file with deletion access rights 62c3...3589	

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1012	Query Registry	Discovery	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more		- Reads information about supported languages 62c3...3589 - Queries the display settings of system associated file extensions 62c3...3589 1 confidential indicators	
T1518.001	Security Software Discovery	Discovery	Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. Learn more		- Possibly checks for the presence of a forensics/monitoring tool 62c3...3589	
T1057	Process Discovery	Discovery	Adversaries may attempt to get information about running processes on a system. Learn more		- Queries process information 62c3...3589	- Observed Process32First/Process32Next/CreateToolhelp32Snapshot API string 62c3...3589
T1497	Virtualization/Sandbox Evasion	- Defense Evasion - Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more	- The input sample contains a known anti-VM trick 62c3...3589		
T1120	Peripheral Device Discovery	Discovery	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Learn more			- Queries volume information 62c3...3589
T1082	System Information Discovery	Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more		- Reads the cryptographic machine GUID 62c3...3589	

Collection

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1074.001	Local Data Staging	Collection	Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Learn more			- Creates a writable file in a temporary directory 62c3...3589
T1114.001	Local Email Collection	Collection	Adversaries may target user email on local systems to collect sensitive information. Learn more	- Reads mail related files 62c3...3589		

Önlemler ve İyileştirmeler

- Önemli verilerinizi düzenli olarak yedekleyin. Yedeklerinizin sisteminizden izole edilmiş olmasına özen gösterin.
- Çalışanlarınızı sosyal mühendislik ve oltalama tekniklerine karşı eğitin.

Kaynakça

- <https://9to5mac.com/2022/07/20/cloudmensis/>
- <https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/>
- https://www.binarydefense.com/threat_watch/cloudmensis-backdoors-mac-users-to-steal-credentials%ef%bf%bc/
- <https://www.bleepingcomputer.com/news/security/new-android-malware-on-google-play-installed-3-million-times/>
- <https://lifel hacker.com/delete-these-sneaky-malware-apps-from-your-android-asap-1849182983>
- <https://twitter.com/IngraoMaxime/status/1547164768401858560>
- <https://www.hybrid-analysis.com/sample/95547426cd892cc50547d65aef7edb82212c68a44257318cb89fbfcfa04889bb?environmentId=200>
- <https://redcanary.com/blog/chromeloder/>
- <https://www.pcrisk.com/removal-guides/23957-chromeloder-malware>
- <https://cyware.com/news/researchers-uncovered-new-variants-of-the-chromeloder-malware-f382ff70>
- <https://unit42.paloaltonetworks.com/chromeloder-malware/>
- <https://www.hybrid-analysis.com/sample/ded20df574b843aaa3c8e977c2040e1498ae17c12924a19868df5b12dee6dfdd>
- <https://www.hybrid-analysis.com/sample/dbac4f2ffcb4e09aad772895647e8f161b1ac713592fe47c5e8207c85722f13>
- <https://www.cisa.gov/uscert/ncas/alerts/aa22-181a>
- <https://id-ransomware.blogspot.com/2019/10/medusalocker-ransomware.html>
- <https://blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/>
- https://twitter.com/JAMESWT_MHT/status/1544946534915219456
- <https://www.hybrid-analysis.com/sample/f3caa040efb298878b99f883a898f76d92554e07a8958e90ff70e7ff3cfabdf5>



INTER PROBE

INTELLIGENCE & ANALYTICS

Mutlukent Mah. Fesleğen Sok. No:9 Çankaya Ankara Türkiye

Phone: +90 312 225 10 93, **Email:** info@interprobe.com.tr, **Web:** <https://interprobe.com.tr>