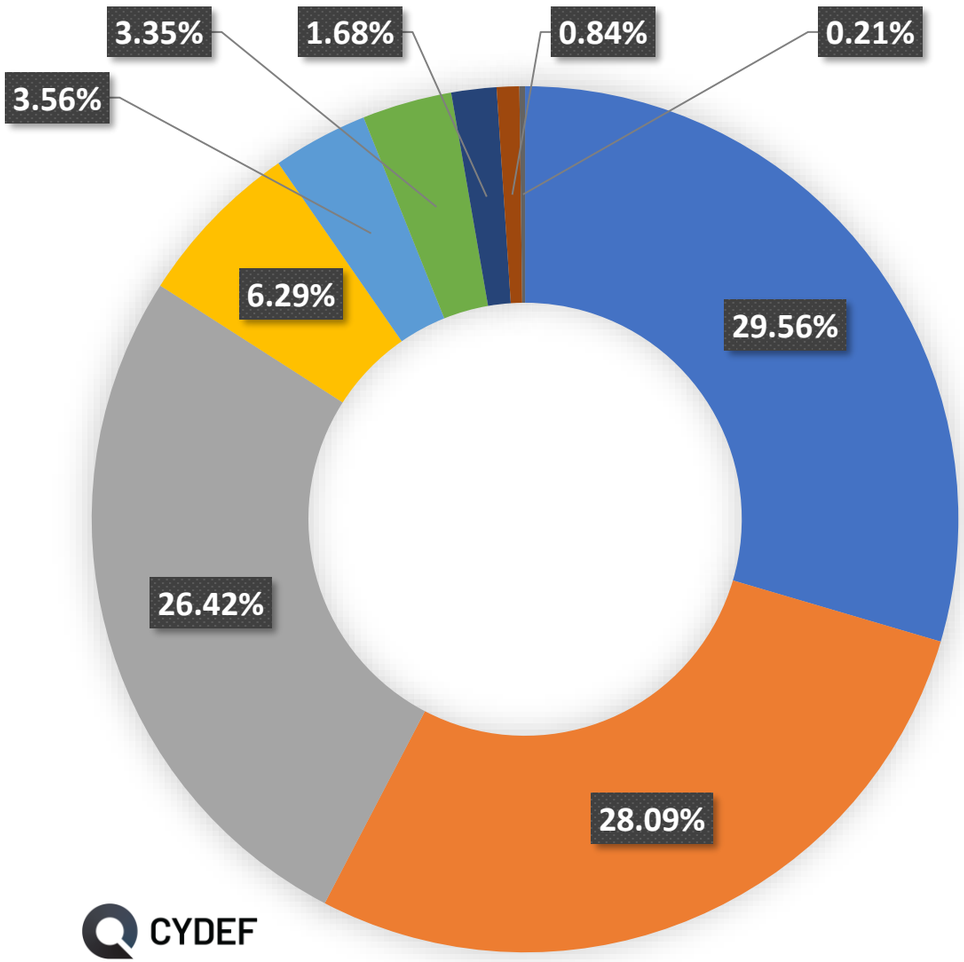
Ejemplo de Reporte de Incidente

Desglose del Incidente



Desglose de incidentes

aplicables a todos los clientes de CYDEF (90 días)

- Software Potencialmente No Deseados (PUP por sus siglas en inglés)
- Informacional
- Violación de Política
- Suplantación de identidad (Phishing)
- Software de comunicaciones (Comms)
- Software malicioso
- Bajo investigación
- Piratería de informática (hacking)
- Secuestro de datos (Ransomware)

Ejemplo de *Tickets* (incidencias)

4. Ataque de Software Malicioso
5. Software Potencialmente No Deseado (PUP) – De Baja Prioridad
6. Software Potencialmente No Deseado (PUP) – De Prioridad Media
7. Usuario con Comportamiento Malicioso
8. Ataque de Secuestro de Datos
9. Ataque Vivir de la Tierra (*Living Off the Land*)

*Algunos elementos de estos *tickets* han sido ocultados.

Ataque de Software Malicioso

SMART-Monitor Alert - HIGH - Malware - Pirated game including additional malware

One of your users downloaded and installed a pirated game on the machine [REDACTED]. The pirated game in questions asked the user to disable security tools (turn off AV, disable auto-updates) and ended up installing a trojan downloader (see VT below). This type of malware downloads further malware components, usually on a pay-per-download basis. This means the machine is likely to receive additional malware payloads in the near future. The malware payloads will not be stopped by the AV since it has been disabled.

We recommend immediately taking the machine off the network and rebuilding it from a clean image. Furthermore, the user in question ([REDACTED]) should reset his password and any access to network resources he had since the compromise should be audited to make sure it is legitimate.

Based on the payloads we have seen up to date, it is unlikely to propagate by itself. We will continue monitoring to make sure that the situation does not change.

VT :
https://www.virustotal.com/gui/file/a45a358e6f4baf873d6d31b6620b30f956bf31fb5e242c8a47fa09ce35f18883/detection

Evidence for the activity (non-exhaustive)
Access to the game bundle
Process Creation
Client: [REDACTED]
ClientGuid: [REDACTED]
Computer Name: [REDACTED]
Device: [REDACTED]
UtcTime:2020-12-16 07:46:31.720
Logon
Account: [REDACTED]
Privileges: Medium
Id:0x29921a8
Child
PID:13036
ProcessGuid:{a6b33d63-bb57-5fd9-6508-000000000f00}
Image: WinRAR.exe
Path:C:\Program Files (x86)\WinRAR
CommandLine:"C:\Program Files (x86)\WinRAR\WinRAR.exe" "F:\Oceanofgames.comDelta_Force2.zip"
Company: Alexander Roshal
Product: WinRAR
Description: WinRAR archiver
Version:5.71.0
MD5:F59F4F7BEA12DD7C8D44F0A717C21C8E
SHA1:
SHA256:F150B01C1CBC540C880DC00D812BCCA1A8ABE1166233227D621408F3E75B57D4
Parent
PID:9144
ProcessGuid:{a6b33d63-97c9-5fd9-7d05-000000000f00}
Image:explorer.exe
Path:C:\Windows
...

Esto demuestra los peligros del software no-autorizado y resalta una investigación a profundidad.

Software Potencialmente No Deseado (PUP) – De Baja Prioridad

SMART-Monitor Alert - Low - Under Investigation - Phenomenon Meteorite CE under investigation

We have detected a new application running from one of your clients. Based on cursory investigation, it seemed like a hidden object game. However, the behavior looked a bit strange. First, it seems to be running from an EasyFileEncryptor folder. Second, it seems to be interacting a bunch with calender.plist which would be unusual for a hidden object game. After doing some more research, we found another program that seemed to have a similar behavior pattern in a sandbox run https://www.joesandbox.com/analysis/352948/0/html

That other program is flagged as adware. If the game we are investigating was also adware, this would explain the interaction with calender and the running from a weird folder.
The program itself currently isn't recognized by VirusTotal. We would recommend uploading it to VT to see if there is any malware detection. Alternatively, if the end customer is complaining about unwanted ads, this would be a prime suspect.


```
{
  "ClientId": "[REDACTED]",
  "ClientName": "[REDACTED]",
  "DeviceId": "[REDACTED]",
  "DeviceName": "[REDACTED]",
  "EventType": "Process Creation",
  "ActivityId": 1422531,
  "SessionId": 100056,
  "User": "[REDACTED]",
  "UtcTime": "2021-08-12T16:25:57.489Z",
  "ParentProcessGuid": "8A0206AB-D904-0000-E8F9-CAE45245D841",
  "LogonId": 501,
  "ProcessId": 1284,
  "ProcessGuid": "8A0206AB-0405-0000-4964-F9E45245D841",
  "ParentProcessId": 1241,
  "ParentImage": "/Users/[REDACTED]/Library/Application
Support/.EasyFileEncryptor/PhenomenonMeteoriteCE",
  "Sha256":
"BF71F6AD4902E0C7C1361CD9DCF61DDA1EA7F111DD013565F8F093930648C6E8
",
  "Image": "/usr/bin/defaults",
  "CommandLine": "sh -c /usr/bin/defaults delete
/Users/[REDACTED]/Library/Preferences/Calender.plist"
}
```


Este es un ejemplo de una investigación en la que encontramos software malicioso sin autenticación y demuestra nuestros altos estándares de servicio a cliente.

Software Potencialmente No Deseado (PUP) – De Prioridad Media

SMART-Monitor Alert - Medium - Potentially Unwanted Program - CompanyUpdater (adware)

When you connected to remove the easyfileencryptor directory, we have observed a new software running (CompanyUpdater). It seems that this software is actually adware that resides in the Lanch agent folder and is actually a piece of adware software that is hardening the rest against removal.
https://www.macobserver.com/tips/quick-tip/macos-check-launchagents-malicious-software/
https://www.sentinelone.com/blog/apples-malware-removal-mrt-tool-update/
We recommend disabling that software and then rescanning the device with a malware scanner and attempt to remove the folder again.


```
{
  "ClientId": "[REDACTED]",
  "ClientName": "[REDACTED]",
  "DeviceId": "[REDACTED]",
  "DeviceName": "[REDACTED]",
  "EventType": "Process Creation",
  "ActivityId": 2108755,
  "SessionId": 100005,
  "ParentProcessId": 1,
  "ParentProcessGuid": "8A0206AB-0100-0000-51DD-4D003051D841",
  "ParentImage": "/sbin/launchd",
  "ProcessGuid": "8A0206AB-827A-0000-F981-94422A52D841",
  "ParentImage": "/sbin/launchd",

  "ProcessGuid": "8A0206AB-827A-0000-F981-94422A52D841",
  "ProcessId": 31362,
  "CommandLine":
"/tmp/[REDACTED]/CompanyUpdater.app/Contents/MacOS/CompanyUpdater
nr",
  "LogonId": 501,
  "User": "barry",
  "UtcTime": "2021-09-20T15:30:18.501Z",
  "Image":
"/private/tmp/[REDACTED]/CompanyUpdater.app/Contents/MacOS/Company
Updater"
}
```


Este es un ejemplo de una técnica de ataque sin archivos en un ambiente macOS.

Usuario con Comportamiento Malicioso

SMART-Monitor Alert - LOW - Informational - User adding himself to the local administrator group

We have seen a user ([REDACTED]) attempting to add themselves to the local administrator group on a machine ([REDACTED]). We cannot confirm if this was successful or not, but can confirm it was at least attempted. From what we can tell, the process chain is explorer.exe (windows UI) -> cmd.exe -> net.exe -> net1.exe. So, the user manually opened a command windows and entered the command.

Please let us know if this is expected behavior or not.

Process Creation

Client: [REDACTED]
ClientGuid: [REDACTED]
Computer Name: [REDACTED]
Device: [REDACTED]
UtcTime:2021-02-08 19:54:13.212
Logon
Account: [REDACTED]
Privileges: Medium
Id:0x104b77
Child
PID:18200
ProcessGuid:{ad23950c-96e5-6021-1804-000000000e00}
Image:net.exe
Path:C:\Windows\System32
CommandLine:net localgroup administrators [REDACTED]/add
Company: Microsoft Corporation
Product: Microsoft® Windows® Operating System
Description: Net Command
Version:10.0.19041.1 (WinBuild.160101.0800)
MD5:0BD94A338EEA5A4E1F2830AE326E6D19
SHA1:
SHA256:9F376759BCBCD705F726460FC4A7E2B07F310F52BAA73CAAAAA124FDDBDF993E
Parent
PID:15904
ProcessGuid:{ad23950c-9697-6021-1304-000000000e00}
Image:cmd.exe
Path:C:\Windows\System32
Command:"C:\windows\system32\cmd.exe"

Este es un ejemplo de una investigación en la que encontramos a un usuario intentando abusar del sistema. Este ataque de alguien interno probablemente no hubiera sido investigado por otros proveedores de Servicios de Detección y Respuesta Administradas (*MDR por sus siglas en inglés*).

Ataque de Secuestro de Datos

SMART-Monitor Alert - High- Cobalt Strike Ransomware Dropper

I've detected some strange behaviors happening on the [REDACTED] device. For example, I'm seeing a remote thread injection from winlogon to cmd (this can allow malicious libraries to run behind the scenes with cmd):


```
{
  "DeviceName": "[REDACTED]",
  "EventType": "Process Injection",
  "UtcTime": "2021-08-24 17:56:03.069",
  "SourceProcessGuid": "{C0FDAA19-D53F-611F-0025-0E0000007000}",
  "SourceProcessId": "4360",
  "SourceImage": "C:\\Windows\\System32\\winlogon.exe",
  "TargetProcessGuid": "{C0FDAA19-32B2-6125-D2A6-0F0000007000}",
  "TargetProcessId": "12756",
  "TargetImage": "C:\\Windows\\System32\\cmd.exe",
  "NewThreadId": "10088",
  "StartAddress": "0x00000000000623A0",
}
```


Also, there was a suspicious, nondescript file creation:


```
{
  "EventType": "File Creation",
  "ActivityId": 25035645,
  "RuleName": "Global Include List For File Creati
  "UtcTime": "2021-08-24 17:56:49.577",
  "ProcessGuid": "{C0FDAA19-D53F-611F-0025-0E00000
  "ProcessId": "4360",
  "Image": "C:\\Windows\\system32\\winlogon.exe",
  "TargetFilename": "C:\\ProgramData\\m.exe",
  "CreationUtcTime": "2021-08-24 17:56:49.577"
}
```


Este es un ejemplo de un ataque precursor de secuestro y salvó al cliente de lo que probablemente hubiera sido una petición de rescate de millones de dólares.

Last but not least, I found a process dump happening. Was this an authorized procdump from the user [REDACTED]?


```
{
  "EventType": "Process Creation",
  "ActivityId": 25035645,
  "RuleName": "-",
  "UtcTime": "2021-08-24 18:00:19.908",
  "ProcessGuid": "{C0FDAA19-33B3-6125-35A7-0F0000007000}",
  "ProcessId": "9364",
  "Image": "C:\\ProgramData\\procdump64.exe",
  "Description": "Sysinternals process dump utility",
  "Product": "ProcDump",
  "Company": "Sysinternals - www.sysinternals.com",
  "OriginalFileName": "procdump",
  "CommandLine": "\"C:\\ProgramData\\procdump64.exe\" -ma lsass.exe -
accepteula lsass.dmp",
  "CurrentDirectory": "C:\\ProgramData\\",
  "User": "NT AUTHORITY\\SYSTEM",
  "TerminalSessionId": "21",
  "IntegrityLevel": "System",
  "Hashes":
"SHA256=E2A7A9A803C6A4D2D503BB78A73CD9951E901BEB5FB450A2821EAF740FC48496"
,
  "ParentProcessGuid": "{C0FDAA19-D53F-611F-0025-0E0000007000}",
  "ParentProcessId": "4360",
  "ParentImage": "C:\\Windows\\System32\\winlogon.exe",
  "ParentCommandLine": "winlogon.exe"
}
```


I will call you to discuss this as I'd like to do a quick threat hunting session if possible.

Ataque Vivir de la Tierra (*Living Off the Land*)

SMARTMonitor Alert - HIGH - Malware - Dridex
We still haven't finished the investigation, but this is 100% malware. Also, we see outbound comms, so this had some execution. As immediate action, we also suggest to block the C&C comms at the boundary if possible

Este es un ejemplo de un software malicioso muy peligroso que utiliza técnicas para “vivir de la tierra” ajena que son difíciles de encontrar con programas de Detección y Respuesta de Puntos Finales (*EDR por sus siglas en inglés*).

Device: [REDACTED]
UtcTime:2020-04-29 15:06:22.990
Account: [REDACTED]
Privileges:Medium
Id:0xa8485
PID:3132
ProcessGuid:{280346e5-97ee-5ea9-0000-001
Image:powershell.exe
Path:c:\windows\system32\windowspowersh
CommandLine:"c:\windows\system32\windo
"&('n'+'al') ('l'+'ss') ('ne'+'w-obje'+'ct') -f;&('na'+
('i'+'o.strea'+'mre'+'ader')((&('l'+'ss')
('io'+'.compr'+'ession.'+'def'+'l'+'a'+'tes'+'tr'+'eam')([system.io.memorystream]
[convert]::frombase64string('jvzzz6s4ev0ro9zit1uzetueh3lgc1tyq9je2hcslgdh0/3vy3dhie
w6deryzzft/puh[REDACTED]//g8='),[system.io.compression.compressionmode]::decom
press)) ,[text.encoding]::utf8)).readtoend( );;.('l'+'sa') (.('l'+'ss')
('io.'+'stream'+'r'+'eader')(.('l'+'ss') ('io'+'.'+'compress'+'ion.gzi'+'pstrea'+'m')((.('l'+'ss')
('io.m'+'emorystre'+'a'+'m') -a
@(,[convert]::frombase64string($b))),[io.compression.compressionmode]::decompress)
)).readtoend()"
Company:Microsoft Corporation
Product:Microsoft® Windows® Operating System
Description:Windows PowerShell
Version:10.0.18362.1 (WinBuild.160101.0800)
MD5:CDA48FC75952AD12D99E526D0B6BF70A
SHA1:
SHA256:908B64B1971A979C7E3E8CE4621945CBA84854CB98D76367B791A6E22B5F6D
53
Parent
PID:8448
ProcessGuid:{280346e5-97ee-5ea9-0000-001045657e0b}
Image:rundll32.exe
Path:c:\windows\system32
Command:rundll32 -s shell32.dll , ,shellexec_rundll "powershell" "&('n'+'al') ('l'+'ss')
('ne'+'w-obje'+'ct') -f;&('na'+'l') ('ls'+'a') ('ie'+'x') -f;&('ls'+'a')(.('ls'+'s')
('i'+'o.strea'+'mre'+'ader')((&('l'+'ss')
('io'+'.compr'+'ession.'+'def'+'l'+'a'+'tes'+'tr'+'eam')([system.io.memorystream]
[convert]::frombase64string('jvzzz6s4ev0ro9zit1uzetueh3lgc1tyq9je2hcslgdh0/3vy3dhie
w6deryzzft/puh//2/p//4yddfpxj2+4cgf//[REDACTED]/ewpm4fbrc4q989h4hq/qei7efb31
mecauqz3w0lkp17a7588nmfxye5b0yvwmxys1f+sy48lm+dxg2lix3242zs96+//g8='),[syste
m.io.compression.compressionmode]::decompress)) ,[text.encoding]::utf8)
).readtoend( );;.('l'+'sa') (.('l'+'ss') ('io.'+'stream'+'r'+'eader')(.('l'+'ss')
('io'+'.'+'compress'+'ion.gzi'+'pstrea'+'m')((.('l'+'ss') ('io.m'+'emorystre'+'a'+'m') -a
@(,[convert]::frombase64string($b))),[io.compression.compressionmode]::decompress)
)).readtoend()"

Network Communication
PID:10520
ProcessGuid:{280346e5-97fd-5ea9-0000-00106ef87e0b}
Image:powershell.exe
Protocol:tcp

Cómo comunicarte con nosotros

¡Contáctanos!

info@cydef.ca

www.cydef.ca

@CydefCorp

bit.ly/CYDEF

Oficinas

Ottawa
1505 Laperriere Ave,
Suite 308
Ottawa, ON K1Z 7T1

Montreal
1134 Sainte-Catherine W.,
Suite 920
Montreal, QC H3B 1H4