hardsecure

CASE STUDY

FORENSIC MALWARE ANALYSIS

R. Acácio de Paiva nº16, 1ºdir,
1700-006 Lisboa, Portugal

www.hardsecure.com
geral@hardsecure.com

ÍNDICE

OBJETIVO

O presente documento tem por objetivo apresentar, de **forma detalhada e com evidências**, **o resultado da análise dos artefactos identificados durante a análise de logs e eventos de segurança** obtidos a partir de computadores do nosso Cliente X, bem como da **forma como ocorreu o vetor de ataque** a 22 de Dezembro de 2020, **no qual comprometeu o acesso aos dados por parte dos utilizadores, através da sua encriptação e destruição (ransomware Le Chiffre, através da encriptação dos ficheiros armazenados nos computadores e servidores** do Cliente X).

ENQUADRAMENTO

A 22 de Dezembro de 2020 a Hardsecure recebe o contacto no Centro de Operações de Segurança, **através da equipa de Monitorização e Controlo de Incidentes de Segurança** uma chamada telefónica do Cliente X com a **informação da existência de máquinas ligadas na sua rede de dados com comportamentos estranhos, bem como problemas no acesso ao serviço de email, situação que já decorria desde a manhã desse dia**.

A **Hardsecure** a partir das 22h40 do **dia do reporte, inicia o processo de investigação do incidente**, através do acesso a uma das máquinas comprometidas, **situação que decorreu durante essa noite**, através da **recolha de evidências e artefactos para análise**, tendo-se **identificado de imediato** que se tratava de um **ataque de ransomware**, devido ao comportamento das máquinas, bem como identificação de ficheiros encriptados.

ESTUDO E ANÁLISE DO VETOR DE ATAQUE

O **ransomware Le Chiffre encriptou os ficheiros armazenados nos computadores e servidores** do Cliente X. Ao contrário de outros ataques por ransomware, o **Le Chiffre não é distribuído pelos métodos mais comuns** (por exemplo, anexos de e-mail fraudulentos, falsas atualizações, trojans, ...), isto é **proliferaram manualmente**. O Hacker executa o ataque ao sistema e executa manualmente um ficheiro executável com malware.
Os ficheiros dos utilizadores então encriptam e Le Chiffre cria um ficheiro em cada pasta contendo ficheiros encriptados. Este ficheiro contém todas as informações sobre a encriptação, conforme seguinte figura onde consta a informação que foi colocada numa das máquinas do Cliente X (este ficheiro é colocado em todas as máquinas comprometidas).

```
hello.

to recover your 3C98T7_LeChiffre files, send any message to:

telegram  messenger:
https://t.me/isres
@isres
or
email:
lechiffre@firemail.cc

reserve method of communication:
email:
lechiffre@mailchuck.com
usually the answer is 1-10min. If there is no answer,
check the spam folder or write from another email where there is no spam filtering.

super reserve method of communication:
bitmessage messenger:
BM-2cTTNY8gzaTxEoPDs9P1jaSRPdit9n8G65
download the messenger: https://bitmessage.org/wiki/Main_Page


in the response, you will receive instructions.

Have a nice day!
```

Fig. 1 – Ficheiro com info do ataque Le Chiffre.

Os ficheiros foram encriptados usando um algoritmo RSA de 1024. **Os utilizadores também recebem nos seus computadores um endereço de e-mail para contactar os hackers onde constam as instruções de pagamento.** O tamanho do resgate é atualmente desconhecido. **Depois de pagar o resgate, os utilizadores supostamente recebem o 'desencriptador'.** Na verdade, o Le Chiffre fornece uma 'modificação nativa' para pagamento. **Os utilizadores são capazes de receber o desencriptador gratuitamente se esperarem seis meses.** Este comportamento é muito incomum para ataques por ransomware. Normalmente, **os utilizadores que não pagam o resgate, perdem os seus ficheiros.**

Este vetor de ataque **Le Chiffre**, partilha **muitas semelhanças com outros ransomware** tais como CryptoLocker, CryptoWall, TeslaCrypt e muitos outros. Embora **Le Chiffre seja distribuído manualmente**, a maioria dos ransomware proliferaram usando redes P2P (por exemplo, Torrents), atualizações de software falsas, e anexos de e-mail com malware.

Foi recomendado pela Hardsecure para o Cliente X **não entrar em contato com os hackers**, bem como **não efetuar o pagamento para obtenção da chave para recuperação dos dados**, uma vez que a pesquisa mostra que não há garantia de que os ficheiros nunca sejam desencriptados mesmo que o resgate seja pago.

ARTEFATOS E EVIDÊNCIAS

Foram analisados perfis com máquinas infetadas, onde se procedeu a **tentativa de limpeza e restauro dos ficheiros com recurso a várias ferramentas de antivírus, EDRs, C&C de forma a tentar efetuar a limpeza do malware.**

Verificamos que, apesar do ataque ter sido identificado no dia 22 de dezembro de 2020, este já estava a ser executado há pelo menos dois dias.

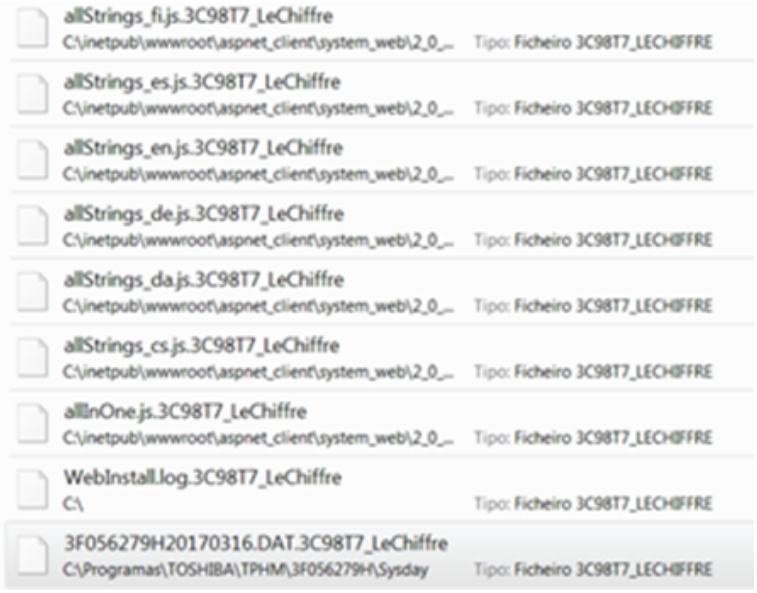


Fig. 2 – Ficheiros encriptados com extensão "lechiffre"

Além disso, através do logon type ID 3 criado na máquina Windows XXX.Cliente X.local identificamos que existiu um logon nesta máquina realizado através da rede as 22h40 hora local (mesma hora em que foi encriptado o ficheiro que constava em outras máquinas), onde através da utilização da conta Cliente X\username (entre outras contas como CLIENTE X\username1) **o hacker acedeu a esta máquina através da rede utilizando o protocolo Server Message Block (SMB), utilizando serviços e protocolos de comunicação com acesso a recursos partilhados** (pastas partilhadas, impressoras, etc).

Através do IP XXX.XX.XX.XXX, utilizando a porta de comunicação 54058 (utilizando o protocolo de encriptação Cryptographic Message Syntax (CMS)), foi utilizada a máquina "workstation" para acesso à máquina XXX.Cliente X.root, com o logon com sucesso nesta máquina, processo idêntico realizado nas restantes máquinas. Desta forma, **o hacker utilizou máquinas como acessos pivots para escalar privilégios** dentro da estrutura do Cliente X, situação realizada sem grandes bloqueios, dado o Cliente X não possuir a sua rede segmentada e segregada ao nível de ACLs e protocolos/serviços, não limitando desta forma a interligação entre VLANs.

Após análise aos logs e eventos de diferentes máquinas, verifica-se a utilização massiva da conta Cliente X\username nos acessos simultâneo a diversas máquinas pelas 21h40 do dia 20 de Dezembro de 2020.

Além disso e utilizando a mesma conta "username", o protocolo Remote Desktop Protocol (RDP) através da porta 3389 foi bloqueado, dado a **existência de ligações já estabelecidas pelo hacker**, onde claramente **bloqueou o acesso a diversos serviços de rede**, tendo também **bloqueado protocolos de comunicação entre as máquinas**, onde existiram diversas sessões estabelecidas entre as máquinas através da utilização de portas encriptadas, conforme ilustra o exemplo a seguir transcrito.

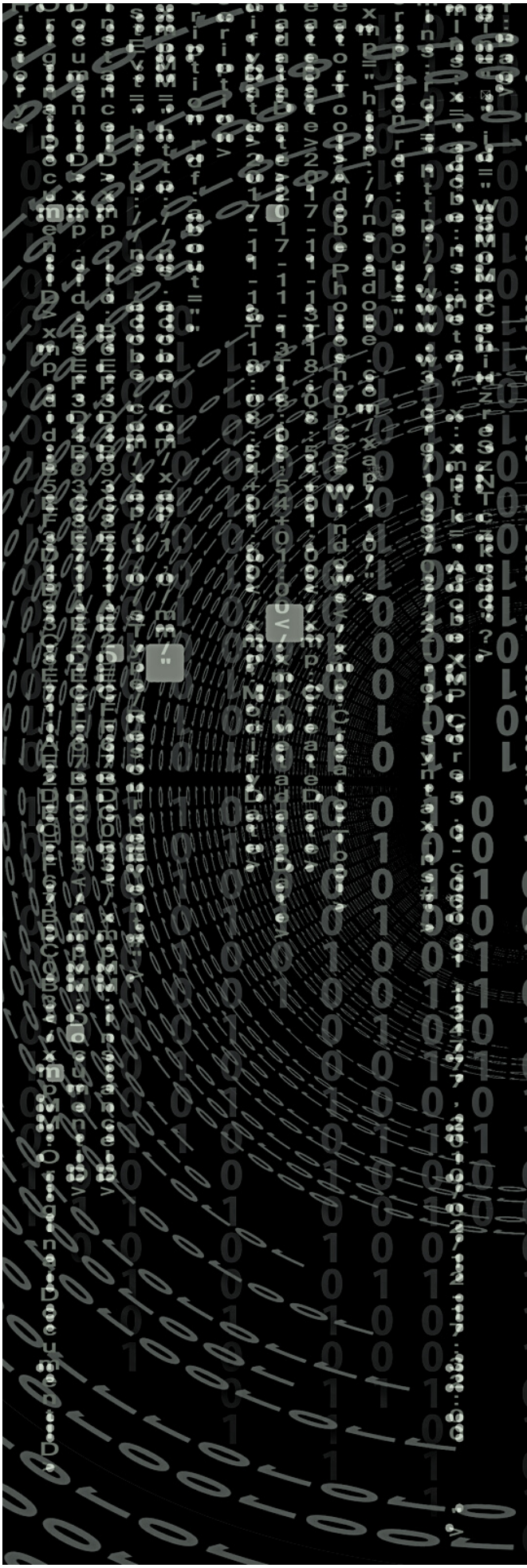
Após análise aos logs das ferramentas de anti-malware utilizadas pelo Cliente X, verifica-se que no dia 17 de Dezembro de 2020 **existiram diversos vetores de ataque via protocolo P2P** (peer – to – peer), através da **utilização desta rede para partilha entre utilizadores, com o intuito de distribuir ficheiros entre todos os nós (os utilizadores) da rede, onde através do modelo de rede-servidor, o computador ou um servidor ficou responsável por armazenar e distribuir os dados entre a rede do Cliente X e o exterior da organização.**

Verificou-se que as **ferramentas não conseguiram bloquear diversas tentativas de ataque** que foram realizadas.

Foram utilizadas diversas ferramentas para ambiente Windows, nomeadamente para identificação de rootkit, malware que invade o sistema e intercepta as funções (API do Windows), conseguindo ocultar a sua presença, intercetando e modificando funções específicas da API. Além disso, **verificou-se que o malware ocultou determinados processos, pastas, ficheiros e chaves de registo, instalando alguns rootkits nos drivers e serviços no sistema** (que também permaneceram "invisíveis" perante os administradores de rede, sistemas e segurança da organização).

```
Damage Cleanup Engine (DCE)  7.5(Build 1137) (RCM: 7.0.0-1176)
Windows 10 Insider Preview(Build 17134)
Start time : sun DEC 17 2020 09:58:24
Load Damage Cleanup Template (DCT) "C:\Program Files (x86)\Trend
Micro\OfficeScan Client\\TMRDCT.ptn" (version ) [fail]
Load Damage Cleanup Template (DCT) "C:\Program Files (x86)\Trend
Micro\OfficeScan Client\\tsc.ptn" (version 1614) [success]
Normal File Check for Detected File "C:\Users\xxx\AppData\Local\WebTorrent\app-
0.23.0\WebTorrent.exe" (Virus Name Unauthorized File Encryption): Normal file
check result 0x00000002, from "WebTorrent LLC [D]".
GenericClean::Pattern:WORM_DOWNAD,Virus Name:Unauthorized File
Encryption,Virus File Path:C:\Users\xxx\AppData\Local\WebTorrent\app-
0.23.0\WebTorrent.exe
GenericClean::Pattern:PE_PATCHEP.A,Virus Name:Unauthorized File
Encryption,Virus File Path:C:\Users\xxx\AppData\Local\WebTorrent\app-
0.23.0\WebTorrent.exe
GenericClean::attern:BKDR_TIDIES,Virus Name:Unauthorized File
Encryption,Virus File Path:C:\Users\xxx\AppData\Local\WebTorrent\app-
0.23.0\WebTorrent.exe
TSC_GENCLEAN[virus found]
-->reboot delete registry
value("HKEY_LOCAL_MACHINE","SYSTEM\CurrentControlSet\services\SharedAcce
ss\Parameters\FirewallPolicy\FirewallRules","TCP Query User{F8569ED7-ACFB-
4A5A-81E0-2DD922E35E9D}C:\users\xxxx\appdata\local\webtorrent\app-
0.23.0\webtorrent.exe") success
-->reboot delete registry
value("HKEY_LOCAL_MACHINE","SYSTEM\CurrentControlSet\services\SharedAcce
ss\Parameters\FirewallPolicy\FirewallRules","UDP Query User{6B1F6282-FAD4-
400E-8FFB-27B575B0350B}C:\users\xxxx\appdata\local\webtorrent\app-
0.23.0\webtorrent.exe") success
 (DCE)  7.5(Build 1137) (RCM: 7.0.0-1176)
Windows 10 Insider Preview(Build 17134)
GenericClean::Pattern:BKDR_PLUGX,Virus Name:Unauthorized File
Encryption,Virus File Path:C:\Users\XXXX\AppData\Local\WebTorrent\app-
0.23.0\WebTorrent.exe
GenericClean::Pattern:LNK_DORKBOT,Virus Name:Unauthorized File
Encryption,Virus File Path:C:\Users\XXXX\AppData\Local\WebTorrent\app-
0.23.0\WebTorrent.exe
```

PROCEDIMENTO DE MITIGAÇÃO



Ações imediatas que foram tomadas:

- Bloqueio de imediato de todas as portas da firewall (exceto VPN com o exterior).

- Levantamento de várias máquinas, tendo como base os seguintes parâmetros de análise:
  - Nome do ativo;
  - IP/Máscara de rede;
  - DNS;
  - Máquina “encriptada” ou “C&C”;
  - Antivírus instalado;
  - Data da infeção;
  - Detalhe do ativo.

Este levantamento permitiu **analisar as máquinas de forma a verificar qual a máquina que deu origem a infeção** (neste caso, a máquina YYYY.Cliente X.local) de forma a **retirá-la de imediato da rede**, dado ser a **máquina que estabelece a comunicação com o exterior** (paciente zero), **bem como ser a fonte de infeção de toda a rede** (além disso, caso esta tivesse a chave instalada na própria máquina, poderia ser recolhida para tentar obter a chave para desencriptação dos dados). Além disso, **este levantamento permitiu-nos determinar quais as máquinas que poderiam ser colocadas numa nova estrutura/rede sem malware, bem como quais os comportamentos que estas apresentam de forma a encontrarmos um padrão que nos permitisse tomar decisões.**

De forma a **apoiar o Cliente X no processo de minimização e bloqueio do malware**, procedeu-se aos seguintes procedimentos:

ETAPA 1
Isolar Máquinas Infetadas.

ETAPA 2
Identificar a infeção e o vetor utilizado para ransomware.

ETAPA 3
Pesquisa de ferramentas de desencriptação do ransomware Le Chiffre.

ETAPA 4
Restauro ficheiros com ferramentas de recuperação de dados.

ETAPA 5
Restauro de cópias de segurança dos dados.

Segue **detalhe das ações** tomadas:

ETAPA 1: ISOLAR MÁQUINAS INFETADAS

Algumas infeções do tipo ransomware são projetadas para encriptar os ficheiros que foram injetados manualmente nas máquinas, infetá-los e até distribuir-se por toda a rede local. Por este motivo, procedeu-se ao i**solamento das máquinas infetadas o mais rápido possível**, através da **criação de uma rede logicamente separada da rede em produção, colocando as máquinas "limpas" nessa rede**.

Além disso, procedeu-se ao **bloqueio no acesso ao serviço de internet** através das máquinas ligadas a rede de dados de forma a garantir que **não continuasse a proliferação do malware por mais máquinas**.

De forma a **garantir que não existissem novamente máquinas comprometidas**, a **Hardsecure iniciou o processo de hardening dos sistemas** (Sistemas operativos, Active Directory & DNS, frameworks de aplicações críticas de negócio, VMs, ativos de rede,...), colocando posteriormente em produção os serviços considerados críticos.

ETAPA 2: IDENTIFICAR A INFEÇÃO E O VETOR UTILIZADO PARA RANSOMWARE

Procedeu-se à **análise forense** relativo ao vetor de ataque em questão. Essa análise, consistiu na **recolha de ficheiros infetados e análise da metodologia de encriptação**, de forma a avaliar se para a realização do ataque o hacker necessitava de um botnet instalado numa máquina da rede do Cliente X para proceder à exfiltração de informação/dados, bem como permitir acessos não autorizados à rede. Desta análise, **verificou-se que o malware era recente sob o nome de Le Chiffre, não tendo sido distribuído pelos métodos mais comuns**, nomeadamente através da utilização de anexos de e-mail com malware, mas sim através da proliferação de comunicação e partilha de rede, com execução manualmente de um ficheiro executável com malware.

ETAPA 3: PESQUISA DE FERRAMENTAS DE DESENCRIPTAÇÃO DO RANSOMWARE LE CHIFFRE

Procedeu-se à **pesquisa junto dos fabricantes**, CIRSTs & CERTs internacionais, Deep Web, Dark Web e outras fontes de informação comerciais e não comerciais, de forma a **identificar possíveis ferramentas e informações** que fossem úteis no sentido de **desencriptar esta versão do ransomware**.

ETAPA 4: RESTAURO FICHEIROS COM FERRAMENTAS DE RECUPERAÇÃO DE DADOS

Relativamente ao processo de **restauro de ficheiros comprometidos**, a Hardsecure efetuou as seguintes tarefas:

- Capacidade total analisada em 7 (sete) discos com informação do Cliente X: 12,54 Terabytes de informação.

- Bloqueio de malware que não foi identificado pelo antivírus ou firewall do Cliente X, mas que apresentava ficheiros com comportamentos irregulares (abertura/fecho de portas, serviços,...): C&C, Botnets, rootkits, trojans (TrojanClicker, TrojanDownloader e TrojanNotifier) e Worms.

- Lista exemplo de ficheiros (com diferentes extensões) identificados com malware (eliminados definitivamente), num total de 2133 ficheiros (não transpomos a totalidade da informação):
  U:\data\DFS_Replication\PR\AdmPP\All\PDF
  U:\data\DFS_Replication\PR\AdmPP\All\vlcmedia-play-2-0-4-win32
  U:\data\flor\Dados\Downloads\awdit-desktop-installer
  U:\data\detalhe\Lisboa\Documentos\trabalho\modeloec.pps

ETAPA 5: RESTAURO DE CÓPIAS DE SEGURANÇA DOS DADOS

O **restauro de backups de informação não foi possível**, dado o Cliente X não possuir esta capacidade tecnológica que permitisse efetuar ao nível dos sistemas (apenas de bases de dados). Esta situação levou a que a **Etapa 4 fosse extremamente demorada e crítica**, levando à Hardsecure empenhar todos os meios a sua disposição, de forma a **garantir recuperação de dados e entrega de dados limpos e sem malware** ao Cliente X, **situação executada com sucesso, contudo com demora.**

CONCLUSÃO

O Cliente X possui um sistema de informação materializado pela descentralização dos seus ativos dos utilizadores por diferentes locais geográficos, centralizado no seu datacenter. O sistema de informação é fundamental para a operacionalização do negócio do Cliente X, onde a prioridade ao longo dos últimos anos destinou-se à operacionalização dos seus sistemas, redes e aplicações, contudo não existiu evolução tecnológica que permitisse uma continuidade e evolução destes sistemas

Os ataques informáticos evoluem a cada instante, as instituições têm dificuldade em acompanhar as constantes mutações e só sentem isto quando efetivamente sofrem um ataque que compromete a sua segurança e imagem perante terceiros.

Este ataque poderia ter tido consequências catastróficas para o Cliente X. Não existindo backups, toda a informação poderia ter sido comprometida e simplesmente o Cliente X deixaria de ter acesso a anos de informação, situação que financeiramente poderia ter sido caótica para a instituição.

A segurança não é visível. O Cliente X teve de orientar o seu esforço para operacionalizar meios de tecnológicos de segurança e humanos de forma a diminuir o risco face à exposição a ataques informáticos.

RECOMENDAÇÕES

De forma a **minimizar e diminuir o risco de exposição a ataques informáticos**, devem os elementos que estão a ler este artigo:

- Proibir que ativos pessoais sejam ligados na rede de dados. Estes ativos, para além da equipa de TI não ter gestão sobre estes, podem possuir malware que é instalado com facilidade na rede de dados.

- Garantir que o antivírus, sistemas operativos, aplicações, bases de dados, frameworks sejam atualizados diariamente, é fundamental para garantir que novos ataques sejam bloqueados e mitigados.

- Garantir que a rede esta segmentada e segregada de forma conveniente, bem como garantir que software/ficheiro seja obtido a partir de fontes fidedignas, de forma a garantir que malware não é propagado por toda a rede de dados.

- Ações de awareness/formação continua a todos os colaboradores da organização. São os utilizadores da rede que, através das suas ações, podem colocar em causa todo um sistema de informação.

- Implementar sistemas de segurança e cibersegurança que garantam uma monitorização, deteção e bloqueio, com resposta a incidentes de segurança.

- Garantir e aplicar políticas de domínio para passwords, conforme as melhores práticas dos standards internacionais de segurança:
  - Com um tamanho mínimo de 14 caracteres;
  - Complexidade, mínimo 1 letra minúscula, 1 letra maiúscula, 1 caracter numérico e 1 caracter especial (não alfanumérico);
  - Expiração de password a cada 30 dias.