[勒索预警]全球最大铝生产商挪威海德鲁遭勒索软件袭击

作者:超弦 AI 攻防实验室

一、 事件概述

欧洲中部时间 2019 年 3 月 19 日， 全球最大铝生产商之一挪威海德鲁(Norsk Hydro)公司 IT 系统遭受一款名为”LockerGoga”的新型勒索软件攻击(该勒索软件首次发现时间为 2019 年 1 月底)，此次攻击涉及其在全球分布的多家铝生产工厂，造成多个工厂临时关闭、部分工厂被迫由”工厂运营模式”切换为”手动运营模式”，给工业生产带来了巨大损失。

挪威海德鲁公司（Norsk Hydro A.S.）创建于 1905 年，现为挪威最大的工业公司，遍布全球 50 个国家，活跃于所有大陆。其在 40 个国家约有 3.5 万名雇员，业务覆盖铝相关全产业链， 据海德鲁公司最新披露，公司在挪威国家安全局以及合作伙伴的帮助下采用工厂隔离、病毒检测与识别、恢复备份系统等方式来遏制病毒传播，目前已基本控制勒索疫情并逐渐恢复生产业务。

六方云超弦实验室在捕获到 LockerGoga 样本后，迅速对其进行了详细分析，并给国内工控企业提供及时预警与防护建议。

二、 样本分析

此样本带有正规证书签名来逃避杀毒软件的查杀，目前该证书已被撤销:

Signature Date 2019-03-23 18:00:00

File Names

tgytutrc
tgytutrc7290.exe

Signature Info

Signature Verification

A certificate was explicitly revoked by its issuer.

File Version Information

Copyright	Copyright (C) ALISA LTD 2019
Product	Service tgytutrc
Description	Background Tasks Host
Original Name	tgytutrc
Internal Name	tgytutrc
File Version	1.5.1.0
Date Signed	6:00 PM 3/23/2019

样本运行后， 会调用 cmd.exe 执行 move 命令，把自身复制到%temp%目录下，文名以硬编码的字符串”tgytutrc”+四位随机数字组成:

c:\windows\system32\cmd.exe	修改文件	C:\Users\Administrator\Desktop\lockergoga.exe
c:\windows\system32\cmd.exe	创建文件	C:\Users\Administrator\AppData\Local\Temp\tgytutrc9388.exe
c:\users\administrator\desktop...	创建新进程	c:\users\administrator\appdata\local\temp\tgytutrc9388.exe

```
v14 = sub_422F10(v13, 0, (unsigned int)"tgytutrc", 8u);
v59 = 0;
v60 = 0;
v58 = *(_QWORD *)v14;
*(_QWORD *)&v59 = *((_QWORD *)v14 + 2);
v14[4] = 0;
v14[5] = 15;
*(_BYTE *)v14 = 0;
LOBYTE(v61) = 2;
HIDWORD(v58) = 4;
DWORD2(v58) = ".exe";
if ( v60 - v59 < 4 )
```

```
DWORD2(v58) = L"cmd.exe";
*(&v62 - 48) = 15;
*((_BYTE *)&v62 - 212) = 0;
*(&v62 - 37) = 0;
*(&v62 - 36) = 7;
*((_WORD *)&v62 - 82) = 0;
sub_418410(DWORD2(v58), HIDWORD(v58));
LOBYTE(v61) = 15;
sub_407930((char *)&v58 + 4);
v38 = (__int16 *)sub_4082E0((LPVOID)DWORD1(v58), DWORD2(v58), HIDWORD(v58));
LOBYTE(v61) = 16;
v39 = sub_433020((int)"/c", (int)(&v62 - 59), (int)&v62);
LOBYTE(v61) = 17;
CopyToTmp(
  v38,                                  // cmd.exe /c move /y C:\Users\Administrator\Desktop\lockergoga.exe %tmp%\tgytutrc9388.exe
  &v62 - 1325,
  (int)&v62,
  a2,
  v39,
  (int)L"move",
  (int)L"/y",
  (int)&dword_51FBC8,
  (int)(&v62 - 29),
  (int)&unk_5022B0);
```

样本启动前会进行反调试，确保自身不在调试环境中:

```
call    ds:IsDebuggerPresent
push    0               ; lpTopLevelExceptionFilter
mov     edi, eax
call    ds:SetUnhandledExceptionFilter
lea     eax, [ebp+ExceptionInfo]
push    eax             ; ExceptionInfo
call    ds:UnhandledExceptionFilter
test    eax, eax
jnz     short loc_4BF39D
```

然后调用 CreateProcessW 以参数”-m”启动(m 为 master process 主进程的意思):

```
if ( a5 == a4 )
{
  sub_41E7A0(&a3, a4, L"-m");
}
else
{
  *(_DWORD *)(a4 + 16) = 0;
  v51[4] = 0;
  v51[5] = 7;
  HIDWORD(v58) = 2;
  *(_WORD *)v51 = 0;
  sub_418410(v51, (int)&v63, (unsigned int)L"-m", HIDWORD(v58));
  a4 += 24;
}
StartRansomware((unsigned int)(&v62 - 29), (int)(&v62 - 1332), (int)&v62, (unsigned int **)&a3, (int)&unk_5022B0);
```

样本启动后会先通过 logoff.exe 注销当前账户并调用 net.exe 修改本地管理员账户密码为样本中硬编码的字符串”HuHuHUHoHo283283@dJD”，

```
mov     byte ptr [ebp-4], 6
push    eax
push    offset aHuhuhuhoho2832 ; "HuHuHUHoHo283283@dJD"
lea     eax, [ebp-2Ch]
push    eax
push    offset aUser    ; "user"
lea     edx, [ebp-74h]
lea     ecx, [ebp-0F4h]
call    ModifyAccountPassword
add     esp, 14h
```

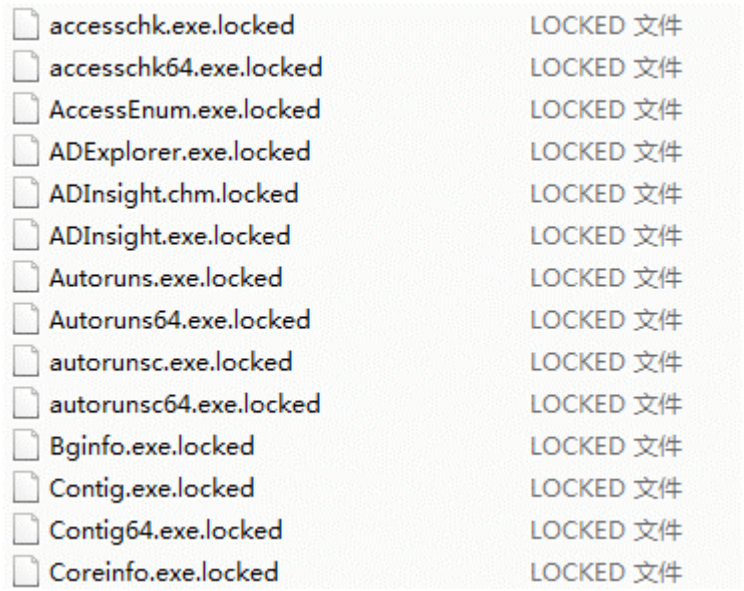
然后开始进行文件加密操作，其会在桌面生成一个名为”README_LOCKED.txt”的勒索信息文件，并开始使用硬编码的公钥对磁盘文件进行加密，加密后的文件后缀为”.locked”：

README_LOCKED.txt - 记事本

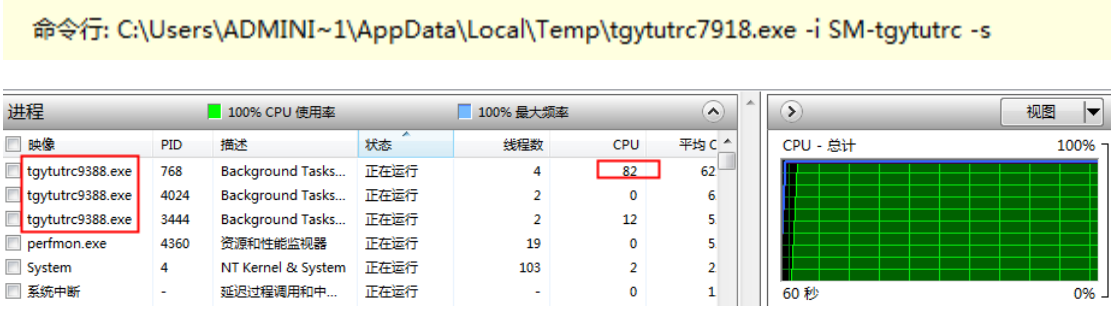
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some
They would have damaged all of your data by mistake or for fun.
Your files are encrypted with the strongest military algorithms RSA4096 and AES-2
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryp
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder de
Sample files we unlock for free (files should not be related to any kind of backu

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

DharmaParrack@protonmail.com
wyattpettigrew8922555@mail.com
```

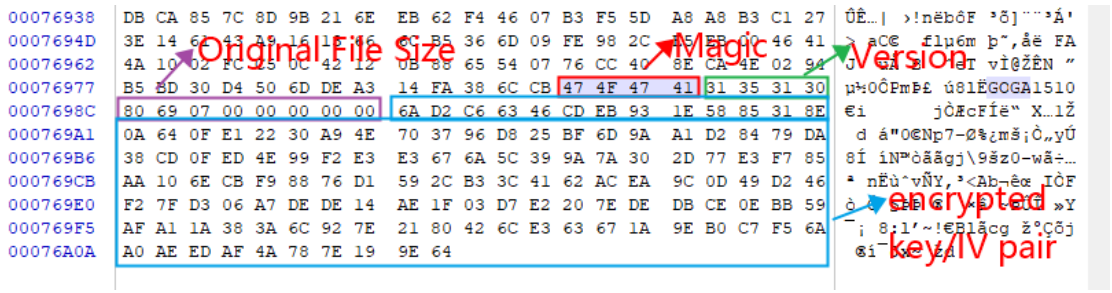
```
sub_409C80(
  &v155,
  (int)" MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDLscAMf6QMU0OLT967Q0oMVN/9xRbC6Ymz HVVE05zgpDJRQQLmPPYcPnehaeynF8HGFYb"
       "RIEaD0pk4WZwGPLtcRaYuQS1M6v+2j4Vp8faA voNdi7+jI2xv0kQao29FJ8WUQDvrPqODALf8bjiOIO7F1Nc5g9vOEbWyCA1w/vbaVwIBEQ==",
  219,
  0);
LOBYTE(v174) = 14;
v12 = sub_41D700(&v170, (int)"InputBuffer", (int)&v155, 1);
LOBYTE(v174) = 15;
((void (__thiscall *)(void ***, void *))v139[8])(&v139, v12);
((void (__thiscall *)(void ***, signed int))v139[50])(&v139, 1);
```



同时样本还会以”-i SM-yxugwjud -s”为参数不断创建子进程进行文件加密，导致样本一运行，CPU 利用率迅速飙升:



“子进程”从共享内存中解码文件路径，使用 RNG(随机数生产器算法)生成 Key/IV(密钥/初始向量)，使用 AES/Rijndael 算法的 CTR 模式(计算器模式)加密文件内容，密钥长度为 128 位，然后使用 RSA-1024 算法加密文件的 Key/IV，样本会把勒索样本魔力字(Magic)、版本(我们捕捉到的样本版本为 1510)、源文件大小、加密后的文件 Key/IV 对附加到加密文件后，如下所示:



经过逆向分析发现，当样本以”-w”参数启动时，将对磁盘所有类型的文件进行加密，而不只局限于样本内置的后缀类型，破坏性较强:

```
aLnk            db '.lnk',0
                align 4
aDoc            db '.doc',0
                align 4
aDot            db '.dot',0
                align 4
aDocx           db '.docx',0
                align 4
aDocb           db '.docb',0
                align 4
aDotx           db '.dotx',0
                align 4
aDotb           db 'dotb',0
                align 4
aWkb            db '.wkb',0
                align 4
aXml            db '.xml',0
                align 4
```

当以”-l”参数启动的时候，样本将会在 C 盘根目录创建一个 log 文件 C:\.log.txt 作为记录:

```
sub_42B3A0((int)&lpMem, a3, a3, (int)"-i", (int)&dword_51FBB0, (int)"-s", &v20, (int)&v21);
LOBYTE(v27) = 0;
v23 = 5;
if ( v26 >= 0x10 )
{
  v9 = lpMem;
  if ( v26 + 1 >= 0x1000 )
  {
    v9 = (_BYTE *)*((_DWORD *)lpMem - 1);
    if ( (unsigned int)((_BYTE *)lpMem - v9 - 4) > 0x1F )
      sub_4BF44B(a2, a3);
  }
  sub_49D2D0(v9);
}
v25 = 0;
v26 = 15;
LOBYTE(lpMem) = 0;
if ( v21 && byte_52A480 )
{
  v18 = &unk_52A4F8;
  v10 = sub_48A3B6(&unk_52A4F8);
  if ( v10 )
    sub_487281(v10);
  v27 = 2;
  sub_414C00(&v17, (int)"c:/.log", 12, v14, v15);
```

.log

```
scanning...
[1/0/53]>C:\Boot\Fonts\chs_boot.ttf
[2/0/53]>C:\360SANDBOX\360SandBox.sav{a8da7be5-8abf-11e6-b977-08002713e4e8}.TMContainer00000000000000000002.regtrans-ms
[1/1/58]+C:\Boot\Fonts\chs_boot.ttf
[2/1/57]>C:\360SANDBOX\360SandBox.sav{a8da7be5-8abf-11e6-b977-08002713e4e8}.TMContainer00000000000000000001.regtrans-ms
[1/1/59]-C:\360SANDBOX\360SandBox.sav{a8da7be5-8abf-11e6-b977-08002713e4e8}.TMContainer00000000000000000001.regtrans-ms
[2/1/58]>C:\FTP\PLC
[1/2/58]+C:\FTP\PLC
[2/2/57]>C:\Boot\memtest.exe
[1/2/58]-C:\360SANDBOX\360SandBox.sav{a8da7be5-8abf-11e6-b977-08002713e4e8}.TMContainer00000000000000000002.regtrans-ms
[2/2/57]>C:\bootmgr
[1/3/58]+C:\Boot\memtest.exe
[2/3/57]>C:\360SANDBOX\360SandBox.sav
[1/4/61]+C:\bootmgr
[2/4/60]>C:\Boot\el-GR\bootmgr.exe.mui
[1/5/91]+C:\Boot\el-GR\bootmgr.exe.mui
```

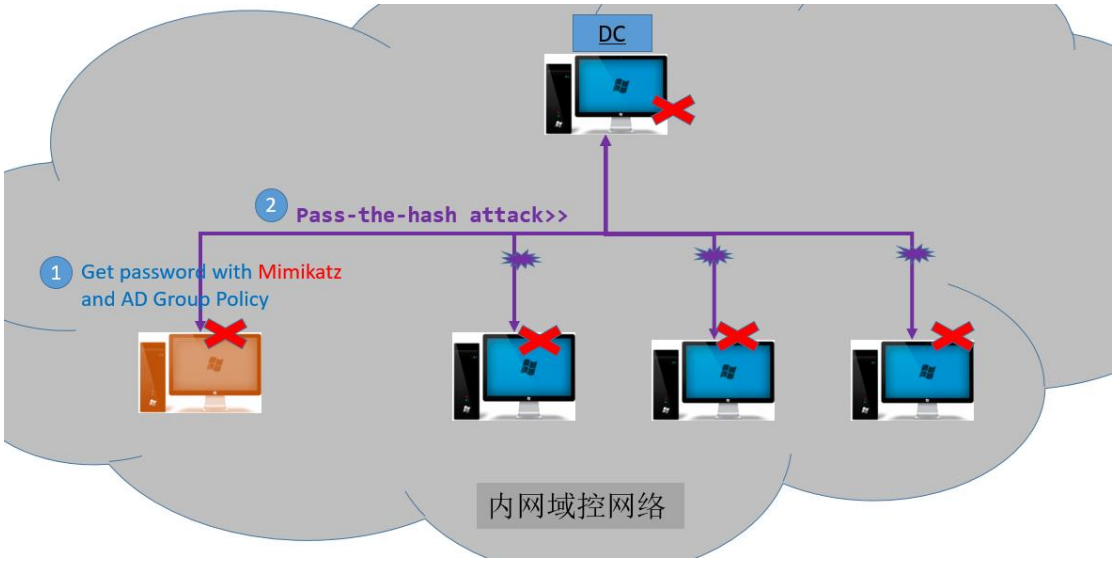
就目前捕捉到的 LockerGoga 勒索版本中，没有发现任何自我传播的代码，这意味着它不会像之前的 Wannacry、NotPety 等勒索蠕虫在网络上自我复制与传播，通过抓包分析也没有发现相关的 C2 以及 DNS 流量，极大的减少其被网络防护设备检测到的可能性，可以推测其主要的目的是破坏，而非间谍活动。挪威计算机应急响应小组(NorCERT)仍在调查此事件，但初步确认该勒索软件可能主要是通过微软 Active Directory(活动目录)进行内网横向传播:

Løsepenge-virus

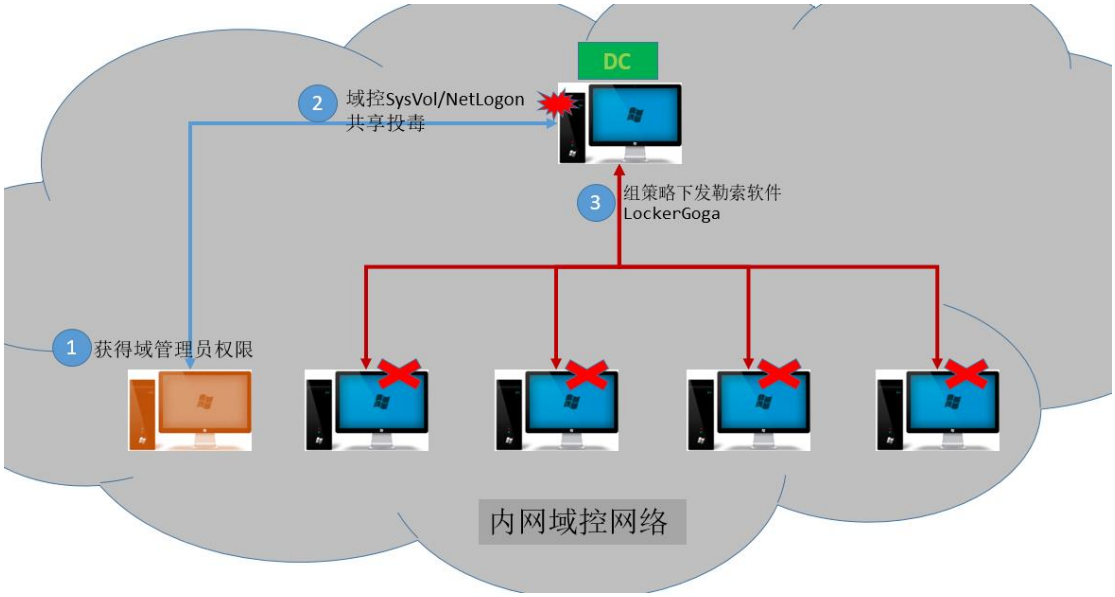
«NorCERT varsler om at Hydro er utsatt for et ransomwareangrep (LockerGoga). Angrepet ble kombinert med et angrep mot Active Directory (AD).

NorCERT ber om informasjon om andre er rammet av tilsvarende hendelser. NorCERT bistår Hydro og hendelsen regnes som pågående», står det i varselet.

可能的攻击流程图如下:



基于上述流程图，攻击者通过 pass the hash 攻击可能获得域管理员权限，这时便可以通过域控共享 SysVol/NetLogon(所有域成员可访问)投毒，然后通过计划任务或服务创建来下发 LockerGoga 勒索实现对所有直连域成员的攻击，进一步的示意图如下:



三、 工控系统勒索软件防护建议

目前没有发现国内企业感染 LockerGoga 勒索软件的迹象，对此六方云超弦实验室提供如下防护建议:

1. 定期对员工进行安全培训，全面提高企业安全意识。
2. 及时更新内网主机系统和应用软件最新补丁，避免存在漏洞
3. 严格管控 U 盘等可移动存储设备的使用，避免内部威胁
4. 更改账户密码为”数字+字母+特殊字符”组成的强密码，并且内网主机避免使用同一密码。
5. 及时备份系统重要数据，提高容灾恢复能力
6. 关闭不必要的服务和端口、文件共享，做好内网域控管理员访问的权限控制
7. 部署杀毒软件、工业卫士(白名单防护软件)、内网威胁管理系统以及工业防火墙等主机和网络层防护措施，全面提高威胁感知

与检测能力

8. 与工控安全厂商合作，定期进行渗透测试与攻防演练，提高应急响应能力

勒索软件重在防护，一旦中招，解密与恢复的可能性十分之小，六方云在这里提醒国内工业企业和厂商一定要做好充足的防护与检测措施，全面提高威胁感知能力，避免遭受巨大的损失。

四、 IoCs

样本哈希:

bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f

88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f

c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15

ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f

eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0

ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f

7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d

723a80c08dd26

C3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a

4b32a053843a

勒索邮箱地址:

MayarChenot@protonmail[.]com

DharmaParrack@protonmail[.]com

SayanWalsworth96@protonmail[.]com

DharmaParrack@protonmail[.]com

wyattpettigrew8922555@mail[.]com

SuzuMcpherson@protonmail[.]com

QicifomuEjijika@o2[.]pl

AsuxidOruraep1999@o2[.]pl

RezawyreEdipi1998@o2[.]pl

AbbsChevis@protonmail[.]com

IjuqodiSunovib98@o2[.]pl

RezawyreEdipi1998@o2[.]pl