Unveiling the Deceptive Dance: Phobos Ransomware Masquerading As VX-Underground

blog.qualys.com/vulnerabilities-threat-research/2023/11/23/unveiling-the-deceptive-dance-phobos-ransomware-masquerading-as-vx-underground

Suraj Mundalik November 23, 2023

During a recent hunt, Qualys Threat Research has come across a ransomware family known as Phobos, impersonating VX-Underground. Phobos ransomware has been knocking on our door since early 2019 and is often seen being distributed via stolen Remote Desktop Protocol (RDP) connections. Strongly believed to be closely tied to the preceding Dharma malware, Phobos usually operates as a Ransomware-as-a-Service (RaaS) threat model.

About VX-Underground

VX-Underground is an open-source community with the largest collection of malware source code, samples, and papers on the internet.
VX-Underground is the most popular source among the threat research community to share malware samples across the globe.

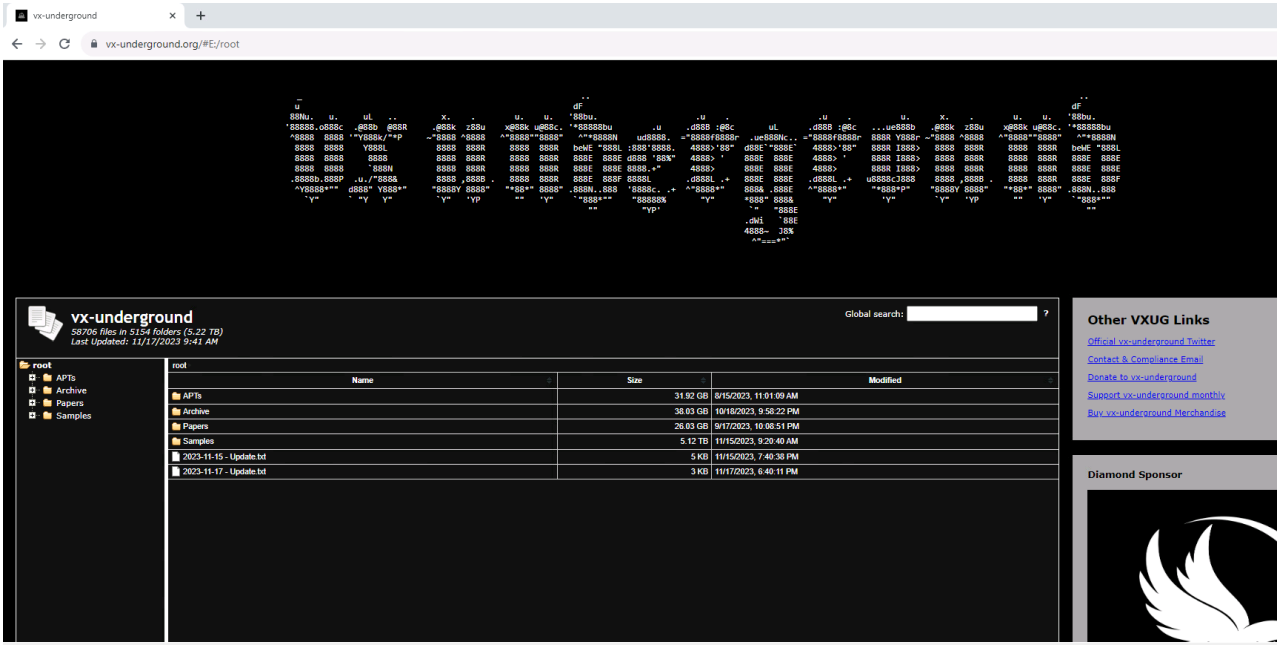

Fig 1. vx-underground

Technical Analysis

AntiRecuvaAndDB.exe (763b04ef2d0954c7ecf394249665bcd71eeafebc3a66a27b010f558fd59dbdeb)

The sample is being distributed with a masqueraded name (AntiRecuvaAndDB.exe) of a legitimate software suite known as Recuva, which is a very popular data recovery software. This file name has been used multiple times in the past by threat actors to distribute malware samples and has recently been seen to be abused by the Phobos ransomware family.

UPX Packed Payload

It is evident that this sample is packed with UPX Packer, as seen in the screenshot below that depicts the sections of the PE file. The binary is compiled for the 32-bit architectures.

property	value	value	value
section	section[0]	section[1]	section[2]
name	UPX0	UPX1	UPX2
footprint > sha256	n/a	A0567E099833015B357CFF0...	B311F19B092A283197543955...
entropy	n/a	7.853	2.763
file-ratio (98.02%)	n/a	96.04 %	1.98 %
raw-address (begin)	0x00000400	0x00000400	0x0000C600
raw-address (end)	0x00000400	0x0000C600	0x0000CA00
raw-size (50688 bytes)	0x00000000 (0 bytes)	0x0000C200 (49664 bytes)	0x00000400 (1024 bytes)
virtual-address	0x00001000	0x0000C000	0x00019000
virtual-size (102400 bytes)	0x0000B000 (45056 bytes)	0x0000D000 (53248 bytes)	0x00001000 (4096 bytes)
characteristics	0xE0000080	0xE0000040	0xC0000040
read	x	x	x
write	x	x	x
execute	x	x	-
share	-	-	-
self-modifying	x	x	-
virtual	x	-	-
items			
directory > import	-	0x00019000	-
base-of-code	0x0000C000	-	-
base-of-data	-	0x00019000	-
entry-point	-	0x00017F50	-

Fig 2. UPX Packed Binary

The Main Culprit – Phobos Ransomware

After unpacking the sample, we can observe the indicators clearly pointing this to be a Phobos ransomware family. Phobos ransomware is very closely related to CrySIS and Dharma malware families and tends to use a UNC Path to access network resources, as seen in the screenshot below.

```
      sub_401110(dwScope, &v6[cCount], (int)a3, a4, a5, a6 - 1);
    }
  }
}
else if ( (v8->dwType & 1) != 0 && sub_4090C6(v8->lpRemoteName) <= 0x8007u )
{
  if ( sub_409216(v6[cCount].lpRemoteName, L"\\\\?\\UNC\\\\\\e-", 8) )
  {
    for ( i = (__int16 *)v6[cCount].lpRemoteName; *i == 92; ++i )
      ;
    sub_408FD7(lpMem, L"\\\\?\\UNC\\\\\\e-", 16);
    sub_40927D((int)lpMem + 16, i);
  }
  else
  {
    sub_40927D((int)lpMem, (__int16 *)v6[cCount].lpRemoteName);
  }
  if ( (int)sub_403711(lpMem) < 0 )
  {
    sub_4035D2(a4);
    v23 = a3[4];
    v21 = a3[3];
```

Fig 3. UNC Path

Phobos halts execution if the Cyrillic alphabets are present on the system, and this is done with the help of native API(s) like GetLocaleInfoW. It checks for the 9th bit, and if the bit is cleared, it detects Cyrillic characters and terminates the infection.

```
dword_40B440 = sub_4062A6(&unk_40B410);
if ( !dword_40B440 )
  return 0;
lpMem = (_BYTE *)sub_406347(49, 0);
TickCount = GetTickCount();
sub_4094FE(TickCount);
if ( (*lpMem & 1) != 0 && GetLocaleInfoW(0x800u, 0x58u, LCData, 32) && (*(_DWORD *)LCData >> 9) & 1 )
  goto LABEL_87;
sub_402876();
v2 = (void *)sub_406347(67, 0);
if ( v2 && !sub_40271B(v2, v33) )
  sub_402876();
sub_4039DA(v2);
```

Fig 4. Cyrillic Detection

The ransomware makes sure that it kills a list of specific processes before it starts its operations, making sure that these processes don't interfere with accessing the files to be encrypted onto the victim system.

The following processes are killed:

"msftesql.exe,sqlagent.exe,sqlbrowser.exe,sqlservr.exe,sqlwriter.exe,oracle.exe,ocssd.exe,dbsnmp.exe,synctime.exe,agntsvc.exe,mydesktopqos.exe,isqlplussvc.exe,xfssvccon.exe,mydesktopservice.exe,ocautoupds.exe,agntsvc.exe,agntsvc.exe,agntsvc.exe,encsvc.exe,firefoxconfig.exe,tbirdconfig.exe,ocomm.exe,mysqld.exe,mysqld-nt.exe,mysqld-opt.exe,dbeng50.exe,sqbcoreservice.exe,excel.exe,infopath.exe,msaccess.exe,mspub.exe,onenote.exe,outlook.exe,powerpnt.exe,steam.exe,thebat.exe,thebat64.exe,thunderbird.exe,visio.exe,winword.exe,wordpad.exe"

```
hSnapshot = CreateToolhelp32Snapshot(2u, 0);
if ( hSnapshot )
{
  sub_408FA9(&pe, 0, 556);
  pe.dwSize = 556;
  if ( Process32FirstW(hSnapshot, &pe) )
  {
    do
    {
      if ( (int)sub_403711(pe.szExeFile) >= 0 )
      {
        v0 = 0;
        v1 = OpenProcess(1u, 0, pe.th32ProcessID);
        v2 = v1;
        if ( v1 )
        {
          v0 = TerminateProcess(v1, 0);
          CloseHandle(v2);
        }
        v6 += v0;
      }
    }
    while ( Process32NextW(hSnapshot, &pe) );
  }
  CloseHandle(hSnapshot);
```

Fig 5. Process Kill Routine

The ransomware tries its best in order inhibit the system recovery by means of executing the following commands:

Delete Shadow Copy

vssadmin delete shadows /all /quiet

wmic shadowcopy delete

Disables automatic Windows Recovery by modifying boot configuration data

bcdedit /set {default} bootstatuspolicy ignoreallfailures

bcdedit /set {default} recoveryenabled no

Delete Windows Backup Catalog

wbadmin delete catalog -quiet

Disable Windows Firewall

netsh advfirewall set currentprofile state off

netsh firewall set opmode mode=disable

Ransomware Artifacts

Once the ransomware payload is executed successfully, it starts the regular encryption routine and encrypts the files on the victim machine with a ".VXUG" extension. Clearly, the threat actor is trying to impersonate VX-Underground by using their shorthand, which is VXUG. The ransomware encrypts and renames the files by appending the following:

.id[unique_id].[staff@vx-underground.org].VXUG

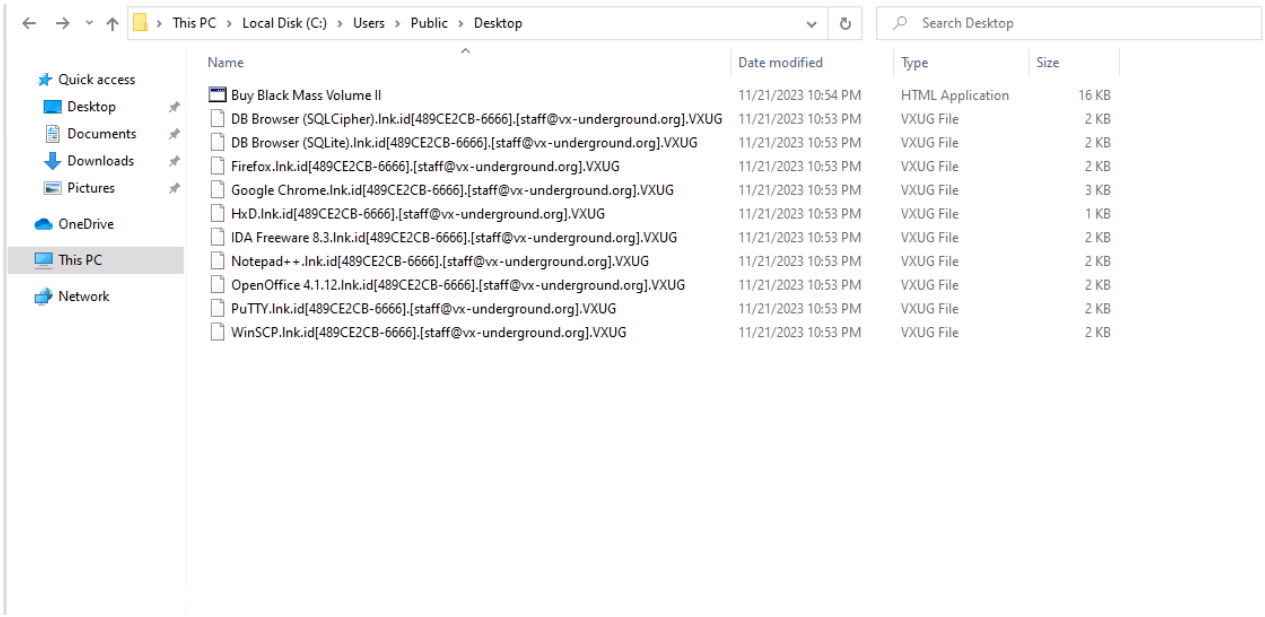

Fig 6. Phobos Encrypted Files

The ransomware achieves persistence by replicating the executable in the Startup directory and adding the Run registry key.

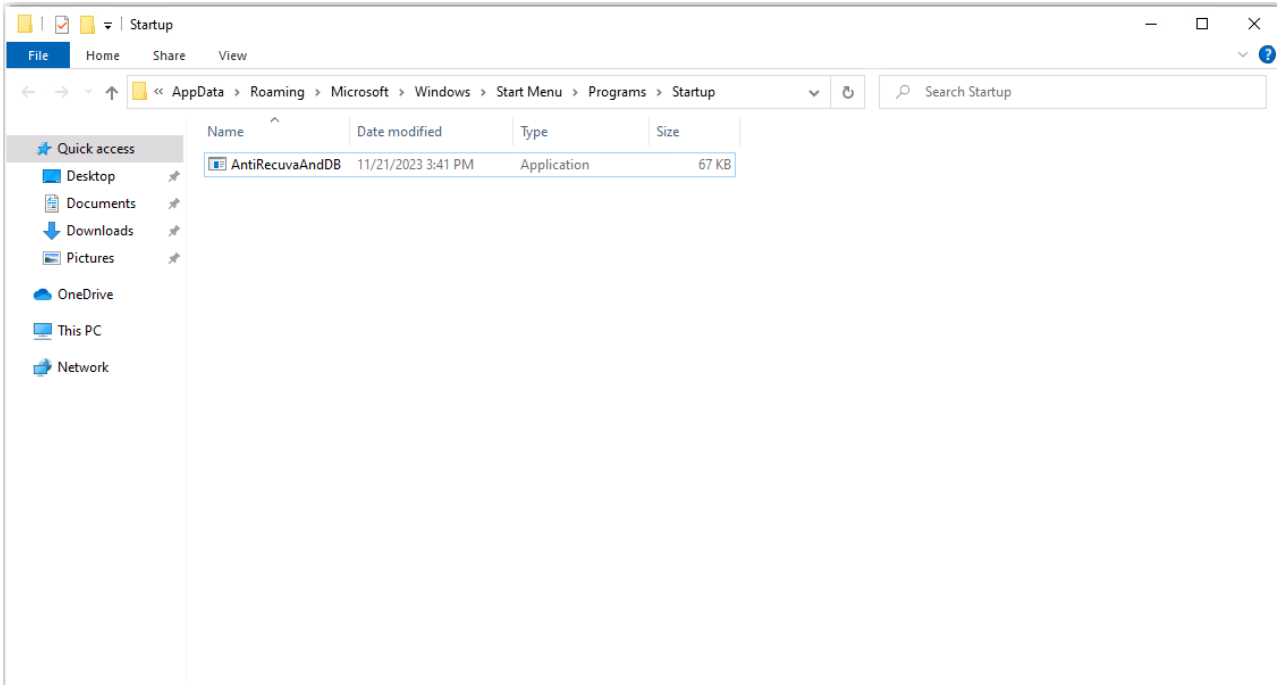

Fig 7. Startup Persistence

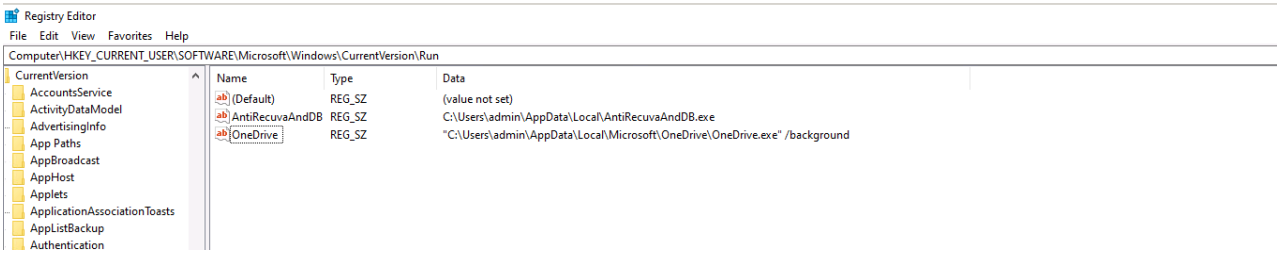

Fig 8. Run Registry Persistence

Phobos also starts dropping the Ransom notes to different directories, starting with the Desktop directory. There are two ransom notes dropped, hta and txt. HTA ransom note is used as a pop-up to push the victim into panic mode.

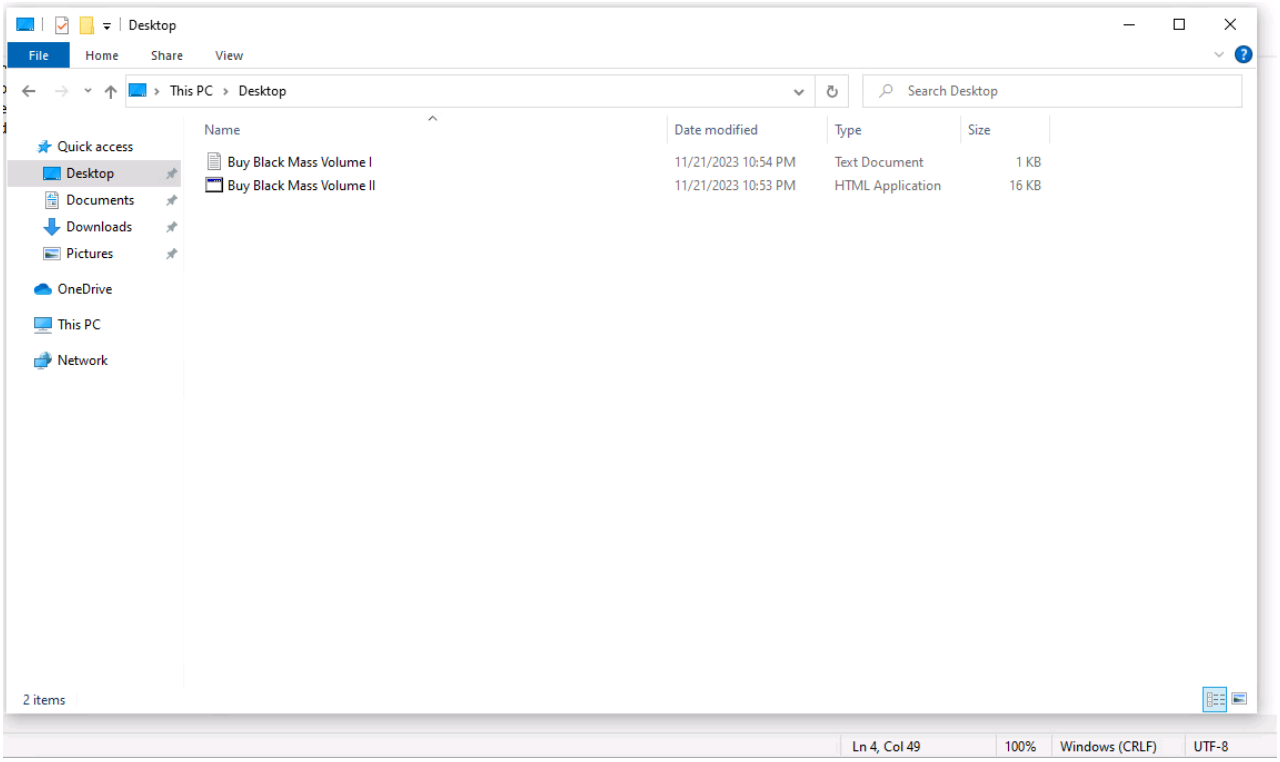

Fig 9. Ransom Notes on Desktop

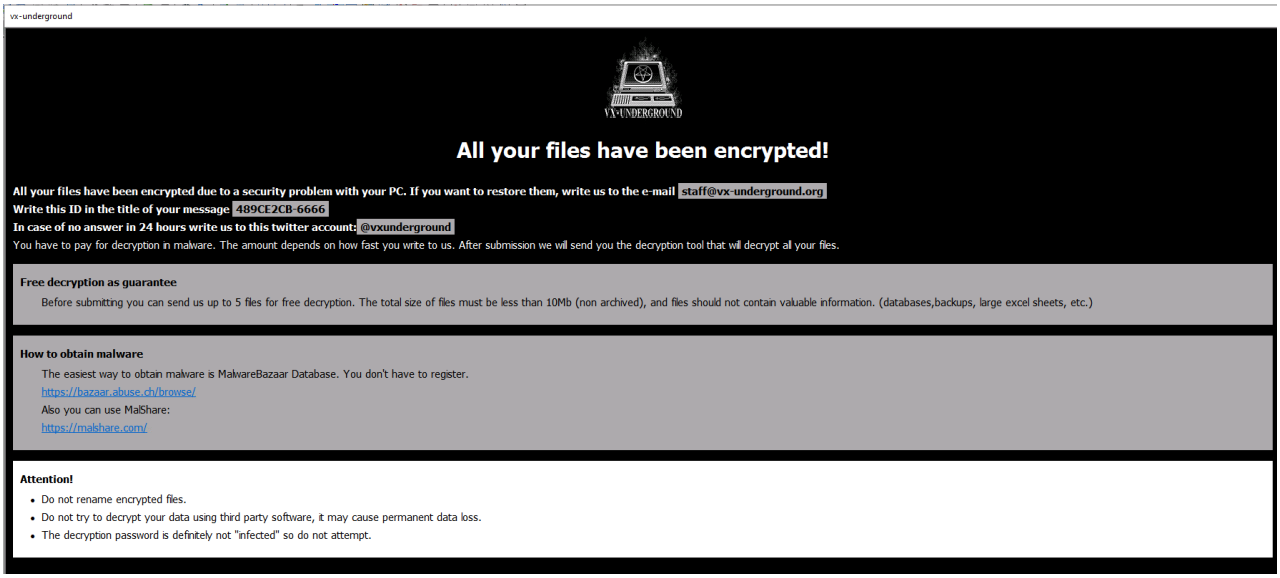

Fig 10. Impersonating Ransom Pop-Up

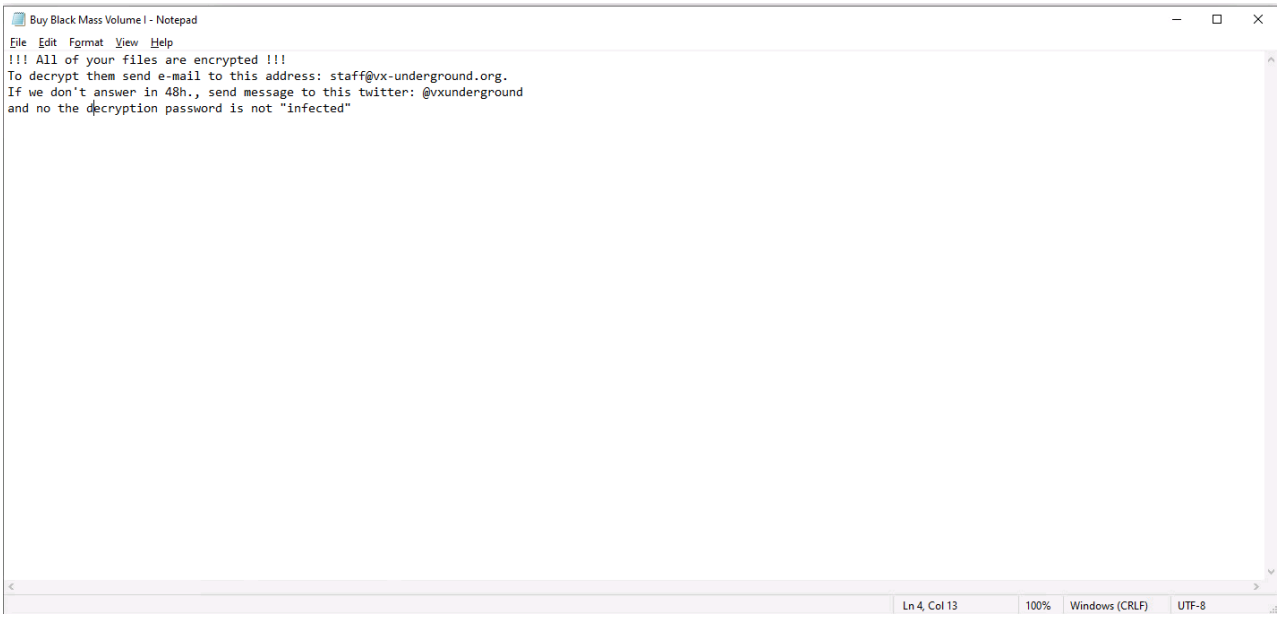

Fig 11. Text Ransom Note

MITRE ATT&CK

Tactic(s)	Technique(s)
Persistence (TA0003)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Privilege Escalation (TA0004)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Defense Evasion (TA0005)	Software Packing (T1027.002) File Deletion (T1070.004) Modify Registry (T1112) Indirect Command Execution (T1202) Disable or Modify Tools (T1562.001)
Discovery (TA0007)	Process Discovery (T1057) File and Directory Discovery (T1083)
Impact (TA0034)	Inhibit System Recovery (T1490)

How Qualys EDR Protects Against These Attacks?

Qualys Threat Research has been proactively monitoring threat actors and their in-the-wild campaigns to deliver the best-in-class detections for all of its customers. Qualys detects this campaign with the following detections:

- Win32.Ransomware.Phobos
- PHOBOS_RANSOMWARE_VX_UNDERGROUND_DISGUISE_T1486
- WMIC_SHADOW_COPY_DELETION_T1490
- DISABLE_AUTOMATIC_WINDOWS_RECOVERY_VIA_BCEDIT_T1490
- DELETE_WINDOWS_BACKUP_CATALOG_T1490
- DISABLE_MICROSOFT_DEFENDER_VIA_REGISTRY_T1562_001
- PHOBOS_RANSOMWARE_VX_UNDERGROUND_DISGUISE_STARTUP_PERSISTENCE_T1547_001

- PHOBOS_RANSOMWARE_VX_UNDERGROUND_DISGUISE_REGISTRY_PERSISTENCE_T1547_001

Hunting queries for This Attack Using Qualys EDR

Qualys EDR customers can use the following hunting queries to look out for any possible indicators of this attack in their environment using the HUNTING tab on the Qualys EDR Cloud Platform:

- file.extension:'VXUG'
- file.fullPath:'\\Desktop\\Buy Black Mass Volume I.txt'
- file.fullPath:'\\Desktop\\ Buy Black Mass Volume II.hta'
- file.fullPath:'\\Windows\\Start Menu\\Programs\\Startup\\AntiRecuvaAndDB.exe'ss
- registry.key:'\\CurrentVersion\\Run' and registry.value:'AntiRecuvaAndDB'

Contributors

Ravindra Deotare, Director, Threat Research, Qualys