Affiliates vs Hunters: Fighting the DarkSide

By Emanuele De Lucia

Published: 2021-01-25 · Archived: 2026-04-05 22:23:58 UTC

Introduction

On **August 2020** a new type of malware, belonging to the *Ransomware* category, appeared in the cyber threat landscape. Threat actor responsible for its development called it "**DarkSide"** and, like others piece of malware of this type, is operated in **Big Game Hunting** (BGH) campaigns. Around more or less the same time, a DLS (**Dedicated Leak Site**) was made available on the *darkweb* (behind the **TOR** network) in order to report the first victims.

On their DLS DarkSide operators claimed to be experienced in conducting cyber operations, having previously used other, not better identified, ransomware variants. Indeed, some characteristics of their first operations support the hypothesis that the group could be a former affiliate of some other **R-a-a-S** (Ransomware as a Service) program that chosen to write their own ransomware likely to avoid sharing the profits of criminal activities with third parties.

Insights

DarkSide is a *well-written* malware family not much changed over the time if compared to the first versions analyzed on August / September 2020. Usually, the samples belonging to this family present some features aimed at making the analysis more harder. For example, in a recent sample (sha256: 17139a10fd226d01738fe9323918614aa913b2a50e1a516e95cced93fa151c61), at **0040182A** we find a ***sub*** aimed at dynamically resolving **DLLs** and **API** through ***LoadLibrary*** / ***GetProcAddress***. ***sub_4016D5***, ***sub_4013DA*** and ***sub_401AC3*** are also involved in this process. The following screenshot shows a chunk of code extracted from the whole function designed for this purpose:

This can be a useful place to create a *code* based **Yara** rule aimed at potentially hunting further variants of the same malware family. After having selected several representative chunks we can obtain something similar to the following:

rule DarkSide_Ransomware_827333_39928 : CRIMEWARE {
meta:
author = “Emanuele De Lucia”
description = “Detects possible variants of DarkSide ransomware”
hash1 = “17139a10fd226d01738fe9323918614aa913b2a50e1a516e95cced93fa151c61”
*/**
call 0x4016d5
push esi
call 0x408195
mov ebx, eax
push dword ptr [esi – 4]push esi
call 0x4013da
mov eax, dword ptr [esi – 4]lea esi, [esi + eax]mov ecx, 0x23
**/*
strings:
$ = { E8 [4] 56 E8 [4] 8B D8 FF 76 ?? 56 E8 [4] 8B 46 ?? 8D 34 06 B9 ?? ?? ?? ?? }
condition:
any of them
}

Darkside employs also techniques for privilege escalation and **UAC** (User Access Control) bypass. The technique observed in this case is known as **CMSTPLUA UAC Bypass** and exploits the **ShellExec** function by

CMSTPLUA COM interface **{3E5FC7F9-9A51-4367-9063-A120244FBEC7}**. This allow to start a process with elevated permissions, according to the following graph:

Powershell is used in order to delete shadow copies preventing the recovery of previously backed up files through them according to the following syntax:

powershell -ep bypass -c
“(0..61)|%{$s+=[char][byte](‘0x’+’4765742D576D694F626A6563742057696E33325F536861646F77
636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'
.Substring(2$_,2))};iex $s”*
Decoded:
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}

A quick **Sigma** rule can be employed in order to hunt for similar *systems-side* behaviors.

title: Detects possible DarkSide infection through PowerShell cmdline used to delete Shadow copies
status: stable
description: Detects possible DarkSide infection through PowerShell cmdline used to delete Shadow copies
author: Emanuele De Lucia
references:
– internal research
tags:
– attack.t1086
– attack.t1064
date: 2020/12/01
logsource:
category: process_creation
product: windows
detection:
selection:
Image|endswith:
– ‘\powershell.exe’
CommandLine|contains|all:
– ‘(0..61)|%%{$s+=[char][byte]’
– ‘4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C

20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'
condition: selection
level: high

Before executing the main payload, the sample performs several other activities like information gathering (f.e. get Disks Info)

and a comparison of system services with a predefined list to stop those ones that could affect the files encryption process

The following are the services malware looks for in the analyzed sample:

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

These areas can likewise be considered in order to extract *bad-known* pieces of code:

rule DarkSide_Ransomware_827333_39929 : CRIMEWARE {
meta:
author = “Emanuele De Lucia”
description = “Detects possible variants of DarkSide ransomware”
hash = “17139a10fd226d01738fe9323918614aa913b2a50e1a516e95cced93fa151c61”
*/**
push 0x10020
push dword ptr [edi]push dword ptr [ebp – 4]call dword ptr [0xcf0e66]mov dword ptr [ebp – 8], eax
cmp dword ptr [ebp – 8], 0
je 0xce4d83
push 0x1c
lea eax, [ebp – 0x30]push eax
call 0xce13da
lea eax, [ebp – 0x30]push eax
push 1
push dword ptr [ebp – 8]call dword ptr [0xcf0e6a]push dword ptr [ebp – 8]call dword ptr [0xcf0e6e]/*

strings:
$ = {68 [4] FF 37 FF 75 ?? FF 15 [4] 89 45 ?? 83 7D [2] 74 ?? 6A ?? 8D 45 ?? 50 E8 [4] 8D 45 ?? 50 6A ?? FF 75 ?? FF 15 [4] FF 75 ?? FF 15 ?? ?? ?? ??}
condition:
any of them
}

After the encryption phase, **Darkside** is designed to communicate to its command and control server in order to share details relating to the victim (victimID) as well as further parameters useful for recovering encrypted files and identifying the affiliate.

Most probably these network capabilities have been added in order to support the R-a-a-S model. In the analyzed sample, the CnC (Command and Control) is attested over the domain name **securebestapp20.com**. Detecting network activities potentially related to this threat could therefore involve writing SNORT rules similar to the following:

alert udp $HOME_NET any -> any 53 (msg:"DNS request for blacklisted domain 'securebestapp20.com'"; content:"|0f|securebestapp20|03|com|00|";nocase; reference:url,https://www.emanueledelucia.net/; sid:[SID HERE]; rev:1;)

This domain name has been created on **16/09/2020** and, according to my visibility, at the time of writing it has a history of **two** (2) A record associated. The interesting one is linked to the IP **185.105.109.19**. Could be interested to note that the **pDNS** count value for this domain name from **21/09/2020** (day of first observed resolution to **185.105.109.19**) to **05/01/2021** (day of last observed resolution to **185.105.109.19**) is less than **180** and that most of them occurred from early November until today. This suggests a growth of the spread and obviously of the **R-a-a-S** business as well. In general, moreover, this number is also consistent with the low overall volume of **DarkSide** campaigns observed at least until mid-November 2020. This is further confirmed by the *payload-side* global visibility I can dispose of for this malware family.

Following are shown detection hits for DarkSide malfamily until the end of the year where it's possible to observe a general increase in the detection rates towards December 2020.

Welcome to Darkside

On **11/10/2020** a user posted an announcement titled "*[Affiliate Program] Darkside Ransomware*" on a **Russian-speaking** darkweb forum. The text contained in that post officially started the project's affiliate program. Press

articles has been used in order to advertise the program itself as well as the skills of the group that are "*aimed only at large corporations*" as originally posted by threat actor itself:

In the affiliate program are not welcome, among others, English speaking personalities, employees of the secret service, security researchers, the greedy (at least so I seem to understand) etc.etc.

There are, moreover, some rules to be respected, like avoiding to target entities within countries belonging to the **CIS** (**Содружество Независимых Государств**), including Georgia and Ukraine, or those operating in education, medicine, public and non-profit sector.

As you might imagine for any other job, there is a selection to go through in order to be included in the program. This includes an ***interview*** to check the candidate's skills and experiences, such having been affiliated with some other program previously. The group offers a **Windows** and **Linux** version of DarkSide ransomware plus an admin panel, a leak site, and a **CDN system** for data storage.

So, do you have ESXi?

At the end of November 2020, a **Linux** variant of **DarkSide** ransomware was uploaded to a *well-known* online malware repository. It had a detection rate, at the time of upload, practically non-existent. Even at time of writing (**Jan 2021**) the detection rate is very low (**2/63**). It seems to have a quite different purpose respect to the Windows counterpart. While the latter is born to encrypt all user files on a workstation (documents, images, PDFs and so on…), the Linux version has been created to damage virtual machines on servers. Indeed, the samples looks for extensions related to **VMWare** files like ***.vmdk***, ***.vmem***, ***.vswp*** and generic logs formats.

The ransom note is similar to the Windows one

and the output of the executable, once launched, confirms the focus on **ESXi** environments

as **/vmfs/volumes/** is the default location of **ESXi** virtual machines. A strict Yara rule similar to the following can help in identifying Linux variants of DarkSide:

rule DarkSide_Ransomware_827333_39930 : CRIMEWARE {
meta:
author = “Emanuele De Lucia”
description = “Detects possible variants of Linux DarkSide ransomware variants”
hash1 = “da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5”
strings:
$ = “vmdk,vmem,vswp,log” fullword ascii
$ = “XChaCha20” fullword ascii
$ = “Partial File Encryption Tool” fullword ascii
$ = “main.log” fullword ascii
condition:
(uint16(0) == 0x457f and all of them)
}

Also for the Linux version, communications to the outside world take place through the same domain name previously reported and a specially crafted URL for each victim. Through Sigma it’s possible to write rules aimed at detecting DNS resolution requests to domain name where actually the command and control is attested:

title: Detects resolution requests to DarkSide Command and Control domain name
status: stable
description: Detects resolution requests to DarkSide Command and Control domain name
references:
– https://www.emanueledelucia.net/fighting-the-darkside-ransomware/
author: Emanuele De Lucia
date: 2020/12/01
tags:
– attack.t1071.001
logsource:
category: dns
detection:
selection:
query:
– ‘securebestapp20.com’

condition: selection
falsepositives:
– internal research
level: high

Adversary Profile

From mid-November 2020, following the affiliation program, it's currently more difficult to associate the exclusive use of **DarkSide** ransomware to a specific threat actor.

However, some similarities with **Revil** suggest that its developer may be familiar with this solution until speculating that it may be from a former Revil affiliate who, to have more control over the operations and not to divide the profits, launched his own project, further enhanced by an independent affiliate program. Regardless the specific actor behind the operations, **DarkSide** can be delivered via several vectors usually after gathering information about the target.

According to my visibility, at least one threat actor who used **DarkSide** adopted the phishing technique (T1566) in order to deliver a *first-stage* payload whose exploitation finally allowed the distribution of DarkSide variants within the victim environment. Other intrusion techniques involve exploiting vulnerabilities in exposed applications (T1190) in order to get a first foothold from which to perform lateral movements.

Indicators of Compromise

Observable	Description	Value
sha256	payload-delivery	da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5
sha256	payload-delivery	17139a10fd226d01738fe9323918614aa913b2a50e1a516e95cced93fa151c61
domain	network-activity	securebestapp20.com

Source: https://socprime.com/blog/affiliates-vs-hunters-fighting-the-darkside/