DarkSide Ransomware Victims Sold Short

mcafee.com/blogs/other-blogs/mcafee-labs/darkside-ransomware-victims-sold-short/

May 14, 2021

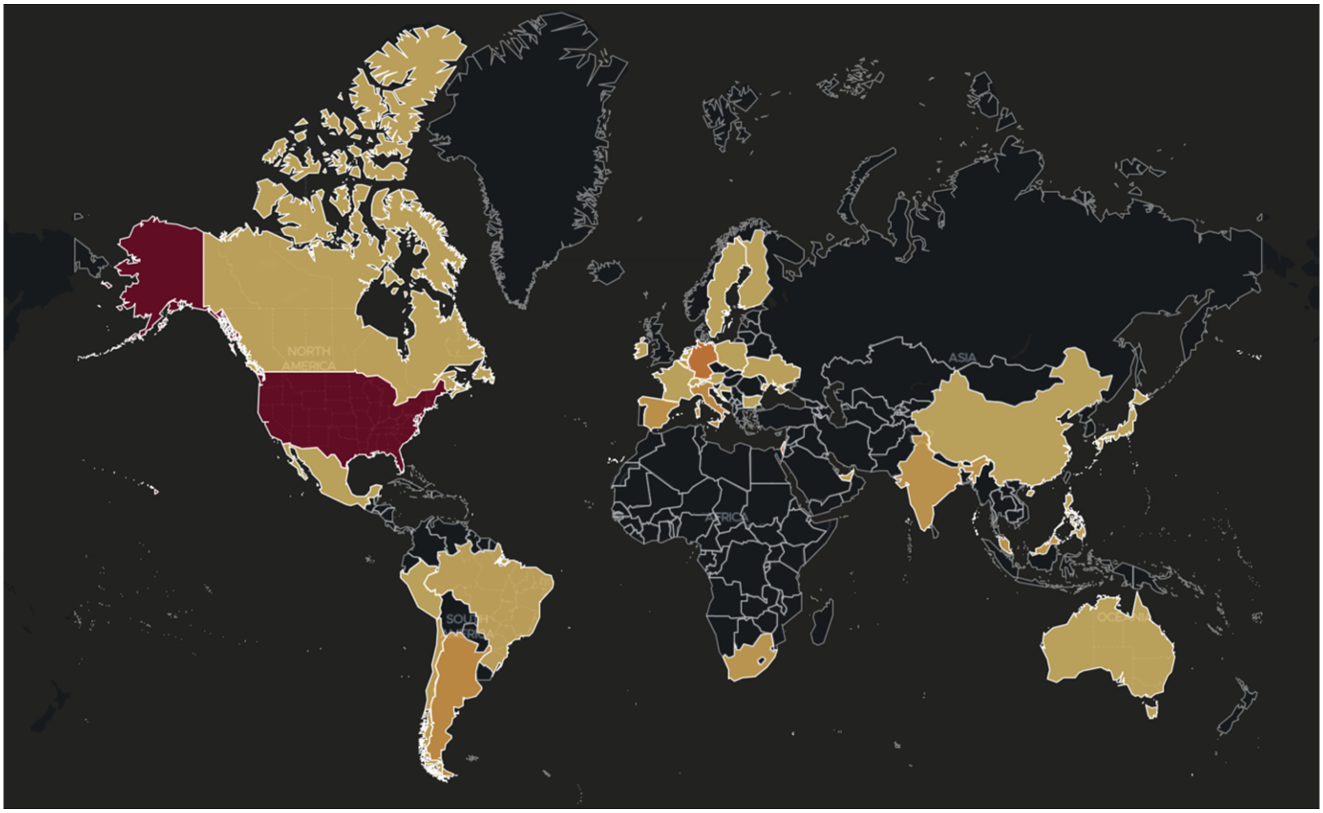
Over the past week we have seen a considerable body of work focusing on DarkSide, the ransomware responsible for the recent gas pipeline shutdown. Many of the excellent technical write-ups will detail how it operates an affiliate model that supports others to be involved within the ransomware business model (in addition to the developers). While this may not be a new phenomenon, this model is actively deployed by many groups with great effect. Herein is the crux of the challenge: while the attention may be on DarkSide ransomware, the harsh reality is that equal concern should be placed at Ryuk, or REVIL, or Babuk, or Cuba, etc. These, and other groups and their affiliates, exploit common entry vectors and, in many cases, the tools we see being used to move within an environment are the same. While this technical paper covers DarkSide in more detail, we must stress the importance of implementing best practices in securing/monitoring your network. These additional publications can guide you in doing so:

- RDP Security Explained: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rdp-security-explained/
- Defending against CUBA Ransomware: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-cuba-ransomware-campaign/
- Ransomware Defenses: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-reality-check-for-your-defenses/
- Building Adaptable Security Architecture Against NetWalker: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-netwalker/
- ENS 10.7 Rolls Back the Curtain on Ransomware: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ens-10-7-rolls-back-the-curtain-on-ransomware/

DarkSide Ransomware: What is it?

As mentioned earlier, DarkSide is a Ransomware-as-a-Service (RaaS) that offers high returns for penetration-testers that are willing to provide access to networks and distribute/execute the ransomware. DarkSide is an example of a RaaS whereby they actively invest in development of the code, affiliates, and new features. Alongside their threat to leak data, they have a separate option for recovery companies to negotiate, are willing to engage with the media, and are willing to carry out a Distributed Denial of Service (DDoS) attack against victims. Those victims who do pay a ransom receive an alert from DarkSide on companies that are on the stock exchange who are breached, in return for their payment. Potential legal issues abound, not to mention ethical concerns, but this information could certainly provide an advantage in short selling when the news breaks.

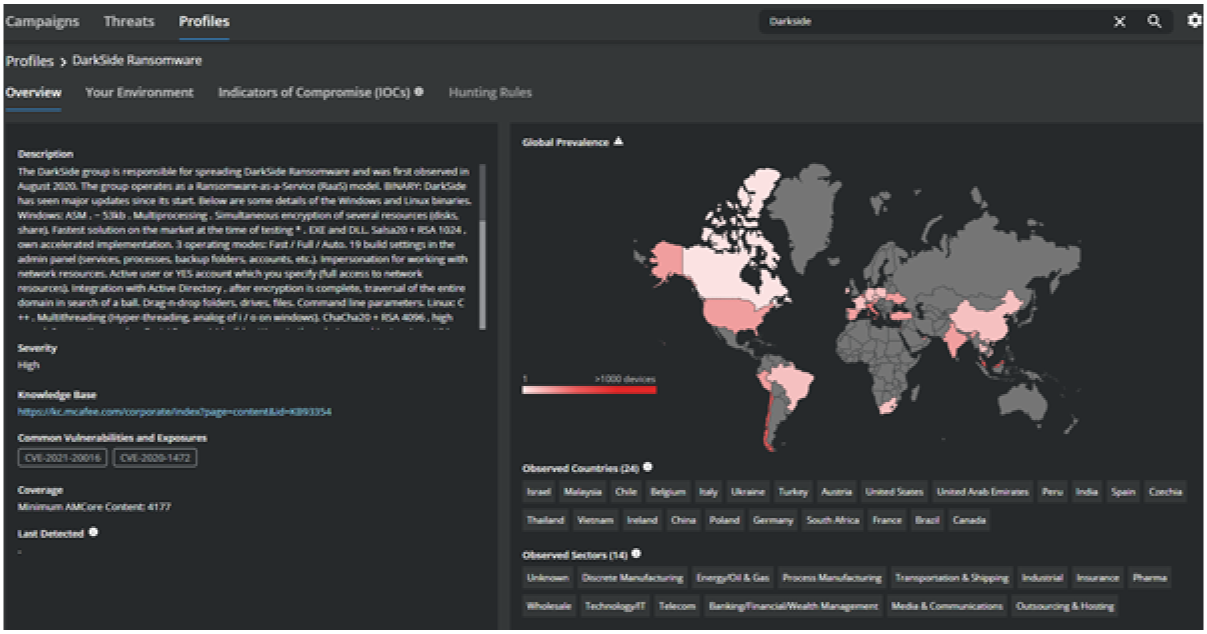
The group behind DarkSide are also particularly active. Using MVISION Insights we can identify the prevalence of targets. This map clearly illustrates that the most targeted geography is clearly the United States (at the time of writing). Further, the sectors primarily targeted are **Legal Services**, **Wholesale**, and **Manufacturing**, followed by the **Oil**, **Gas** and **Chemical** sectors.



Coverage and Protection Advice

McAfee's market leading EPP solution covers DarkSide ransomware with an array of early prevention and detection techniques.

Customers using MVISION Insights will find a threat-profile on this ransomware family that is updated when new and relevant information becomes available.



Description

The DarkSide group is responsible for spreading DarkSide Ransomware and was first observed in August 2020. The group operates as a Ransomware-as-a-Service (RaaS) model. BINARY: DarkSide has seen major updates since its start. Below are some details of the Windows and Linux binaries. Windows: ASM , ~ 53kb , Multiprocessing , Simultaneous encryption of several resources (disks, share). Fastest solution on the market at the time of testing * , EXE and DLL. Salsa20 + RSA 1024 , own accelerated implementation. 3 operating modes: Fast / Full / Auto. 19 build settings in the admin panel (services, processes, backup folders, accounts, etc.). Impersonation for working with network resources. Active user or YES account which you specify (full access to network resources). Integration with Active Directory , after encryption is complete, traversal of the entire domain in search of a ball. Drag-n-drop folders, drives, files. Command line parameters. Linux: C ++ , Multithreading (Hyper-threading, analog of i / o on windows). ChaCha20 + RSA 4096 , high

Severity

High

Knowledge Base

https://kc.mcafee.com/corporate/index?page=content&id=KB93354

Common Vulnerabilities and Exposures

CVE-2021-20016 CVE-2020-1472

Coverage

Minimum AMCore Content: 4177

Last Detected

-

Observed Countries (24)

Israel, Malaysia, Chile, Belgium, Italy, Ukraine, Turkey, Austria, United States, United Arab Emirates, Peru, India, Spain, Czechia, Thailand, Vietnam, Ireland, China, Poland, Germany, South Africa, France, Brazil, Canada

Observed Sectors (14)

Unknown, Discrete Manufacturing, Energy/Oil & Gas, Process Manufacturing, Transportation & Shipping, Industrial, Insurance, Pharma, Wholesale, Technology/IT, Telecom, Banking/Financial/Wealth Management, Media & Communications, Outsourcing & Hosting

Early Detection

MVISION EDR includes detections on many of the behaviors used in the attack including privilege escalation, malicious PowerShell and CobaltStrike beacons, and visibility of discovery commands, command and control, and other tactics along the attack chain. We have EDR telemetry indicating early detection before the detonation of the Ransomware payload.

Prevention

ENS TP provides coverage against known indicators in the latest signature set. Updates on new indicators are pushed through GTI.

ENS ATP provides behavioral content focusing on proactively detecting the threat while also delivering known IoCs for both online and offline detections.

ENS ATP adds two (2) additional layers of protection thanks to JTI rules that provide attack surface reduction for generic ransomware behaviors and RealProtect (static and dynamic) with ML models targeting ransomware threats.

For the latest mitigation guidance, please review:

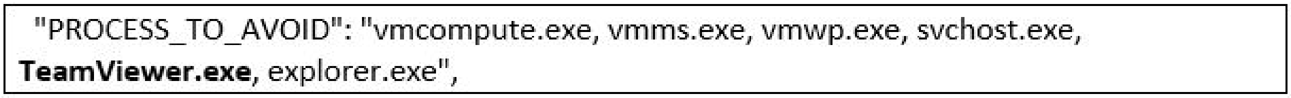
https://kc.mcafee.com/corporate/index?page=content&id=KB93354&locale=en_US

Technical Analysis

The RaaS platform offers the affiliate the option to build either a Windows or Unix version of the ransomware. Depending on what is needed, we observe that affiliates are using different techniques to circumvent detection, by masquerading the generated Windows binaries of DarkSide. Using several packers or signing the binary with a certificate are some of the techniques used to do so.

As peers in our industry have described, we also observed campaigns where the affiliates and their hacking crew used several ways to gain initial access to their victim's network.

1. Using valid accounts, exploit vulnerabilities on servers or RDP for initial stage
2. Next, establish a beachhead in the victim's network by using tools like Cobalt-Strike (beacons), RealVNC, RDP ported over TOR, Putty, AnyDesk and TeamViewer. **TeamViewer** is what we also see back in the config of the ransomware sample:

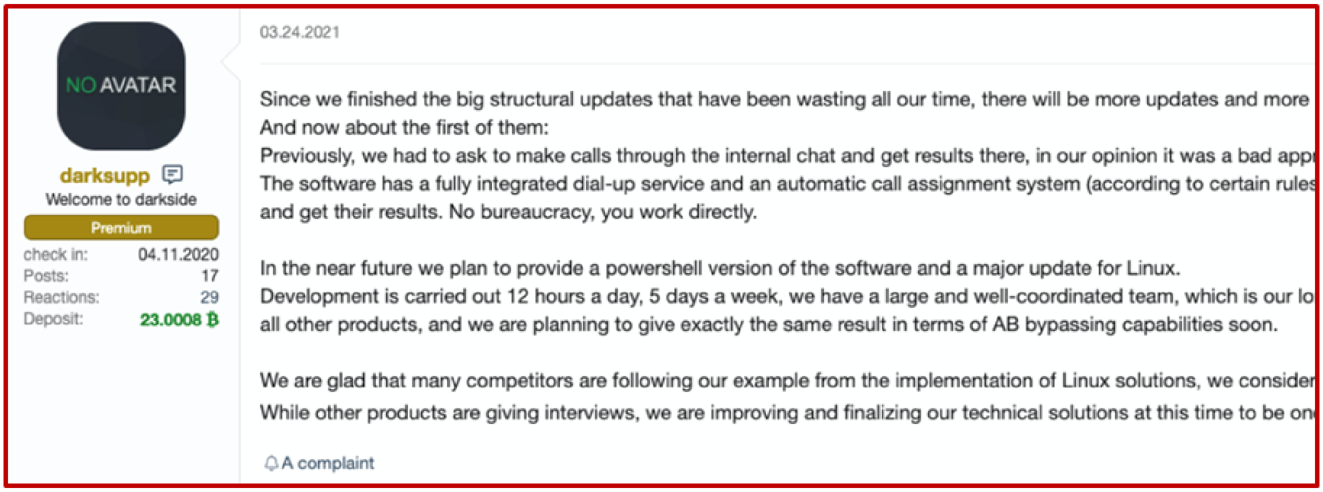


```
  "PROCESS_TO_AVOID": "vmcompute.exe, vmms.exe, vmwp.exe, svchost.exe,
TeamViewer.exe, explorer.exe",
```

The configuration of the ransomware contains several options to enable or disable system processes, but also the above part where it states which processes should not be killed.

As mentioned before, a lot of the current Windows samples in the wild are the 1.8 version of DarkSide, others are the 2.1.2.3 version. In a chat one of the actors revealed that a V3 version will be released soon.

On March 23rd, 2021, on XSS, one of the DarkSide spokespersons announced an update of DarkSide as a PowerShell version and a major upgrade of the Linux variant:


NO AVATAR

darksupp

Welcome to darkside

Premium

check in:	04.11.2020
Posts:	17
Reactions:	29
Deposit:	23.0008 ₿

03.24.2021

Since we finished the big structural updates that have been wasting all our time, there will be more updates and more
And now about the first of them:
Previously, we had to ask to make calls through the internal chat and get results there, in our opinion it was a bad app
The software has a fully integrated dial-up service and an automatic call assignment system (according to certain rules
and get their results. No bureaucracy, you work directly.

In the near future we plan to provide a powershell version of the software and a major update for Linux.
Development is carried out 12 hours a day, 5 days a week, we have a large and well-coordinated team, which is our lo
all other products, and we are planning to give exactly the same result in terms of AB bypassing capabilities soon.

We are glad that many competitors are following our example from the implementation of Linux solutions, we consider
While other products are giving interviews, we are improving and finalizing our technical solutions at this time to be on

A complaint

In the current samples we observe, we do see the PowerShell component that is used to delete the Volume Shadow copies, for example.

1. Once a strong foothold has been established, several tools are used by the actors to gain more privileges.

Tools observed:

- Mimikatz
- Dumping LSASS
- IE/FireFox password dumper
- Powertool64
- Empire
- Bypassing UAC

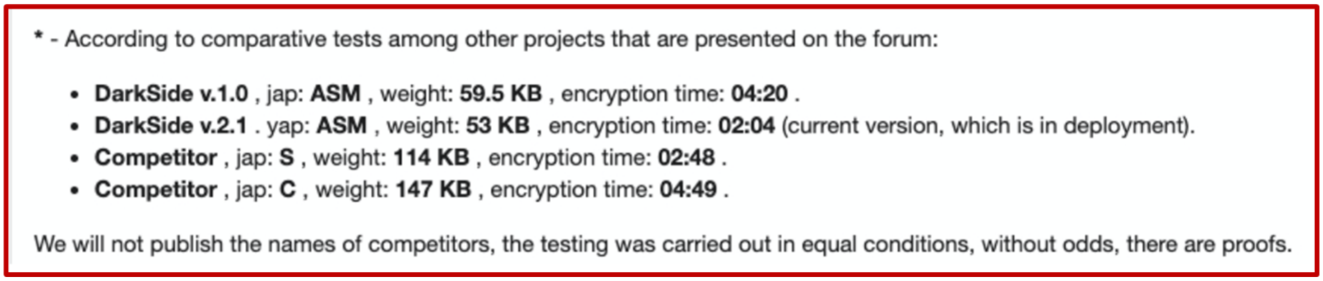
1. Once enough privileges are gained, it is time to map out the network and identify the most critical systems like servers, storage, and other critical assets. A selection of the below tools was observed to have been used in several cases:

- BloodHound
- ADFind
- ADRecon

- IP scan tools
- Several Windows native tools
- PowerShell scripts

Before distributing the ransomware around the network using tools like PsExec and PowerShell, data was exfiltrated to Cloud Services that would later be used on the DarkSide Leak page for extortion purposes. Zipping the data, using Rclone or WinSCP are some of the examples observed.

While a lot of good and in-depth analyses are written by our peers, one thing worth noting is that when running DarkSide, the encryption process is fast. It is one of the areas the actors brag about on the same forum and do a comparison to convince affiliates to join their program:



* - According to comparative tests among other projects that are presented on the forum:

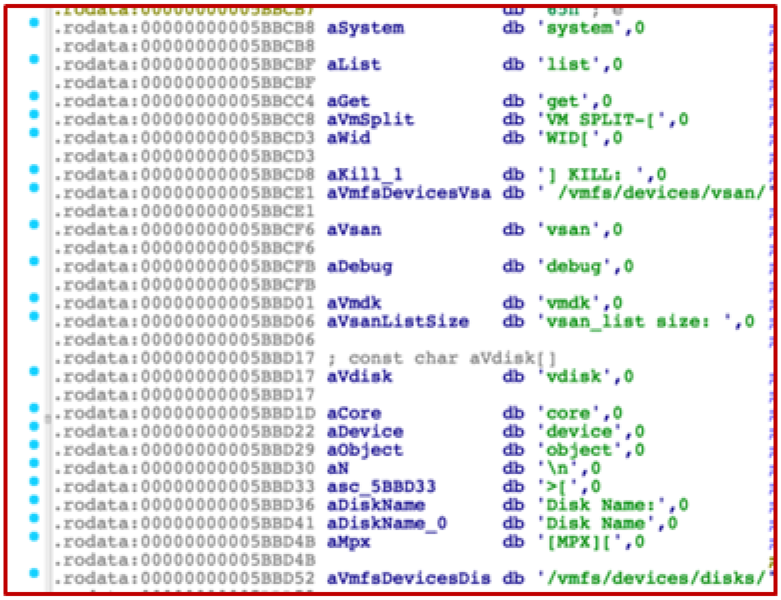
- **DarkSide v.1.0** , jap: **ASM** , weight: **59.5 KB** , encryption time: **04:20** .
- **DarkSide v.2.1** . yap: **ASM** , weight: **53 KB** , encryption time: **02:04** (current version, which is in deployment).
- **Competitor** , jap: **S** , weight: **114 KB** , encryption time: **02:48** .
- **Competitor** , jap: **C** , weight: **147 KB** , encryption time: **04:49** .

We will not publish the names of competitors, the testing was carried out in equal conditions, without odds, there are proofs.

DarkSide, like Babuk ransomware, has a Linux version. Both target *nix systems but in particular VMWare ESXi servers and storage/NAS. Storage/NAS is critical for many companies, but how many of you are running a virtual desktop, hosted on a ESXi server?

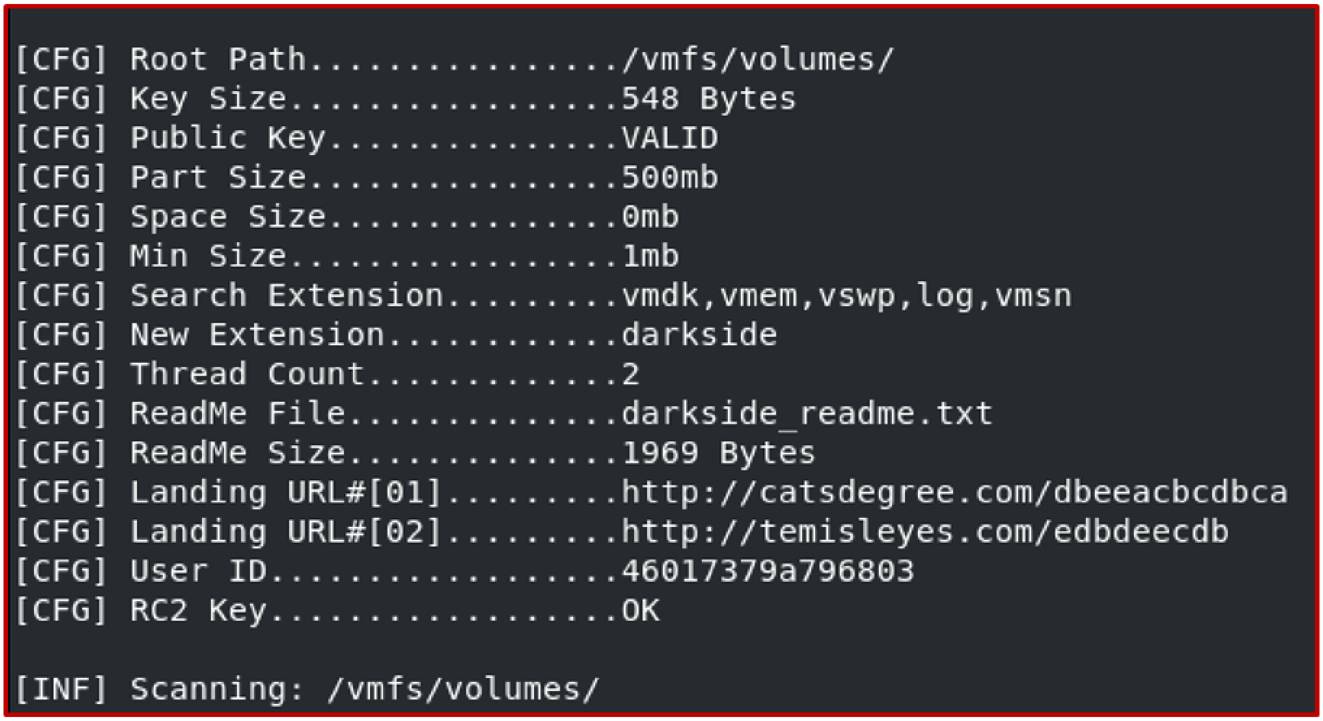
Darkside wrote a Linux variant that supports the encryption of ESXI server versions 5.0 – 7.1 as well as NAS technology from Synology. They state that other NAS/backup technologies will be supported soon.

In the code we clearly observe this support:



```
.rodata:00000000005BBCB7                 db  65h ; e
.rodata:00000000005BBCB8 aSystem         db 'system',0
.rodata:00000000005BBCB8
.rodata:00000000005BBCBF aList           db 'list',0
.rodata:00000000005BBCBF
.rodata:00000000005BBCC4 aGet            db 'get',0
.rodata:00000000005BBCC8 aVmSplit        db 'VM SPLIT-[',0
.rodata:00000000005BBCD3 aWid            db 'WID[',0
.rodata:00000000005BBCD3
.rodata:00000000005BBCD8 aKill_1         db '] KILL: ',0
.rodata:00000000005BBCE1 aVmfsDevicesVsa db ' /vmfs/devices/vsan/'
.rodata:00000000005BBCE1
.rodata:00000000005BBCF6 aVsan           db 'vsan',0
.rodata:00000000005BBCF6
.rodata:00000000005BBCFB aDebug          db 'debug',0
.rodata:00000000005BBCFB
.rodata:00000000005BBD01 aVmdk           db 'vmdk',0
.rodata:00000000005BBD06 aVsanListSize   db 'vsan_list size: ',0
.rodata:00000000005BBD06
.rodata:00000000005BBD17 ; const char aVdisk[]
.rodata:00000000005BBD17 aVdisk          db 'vdisk',0
.rodata:00000000005BBD17
.rodata:00000000005BBD1D aCore           db 'core',0
.rodata:00000000005BBD22 aDevice         db 'device',0
.rodata:00000000005BBD29 aObject         db 'object',0
.rodata:00000000005BBD30 aN              db '\n',0
.rodata:00000000005BBD33 asc_5BBD33      db '>[',0
.rodata:00000000005BBD36 aDiskName       db 'Disk Name:',0
.rodata:00000000005BBD41 aDiskName_0     db 'Disk Name',0
.rodata:00000000005BBD4B aMpx            db '[MPX][',0
.rodata:00000000005BBD4B
.rodata:00000000005BBD52 aVmfsDevicesDis db '/vmfs/devices/disks/'
```

Also, the configuration of the Linux version shows it is clearly looking for Virtual Disk/memory kind of files:

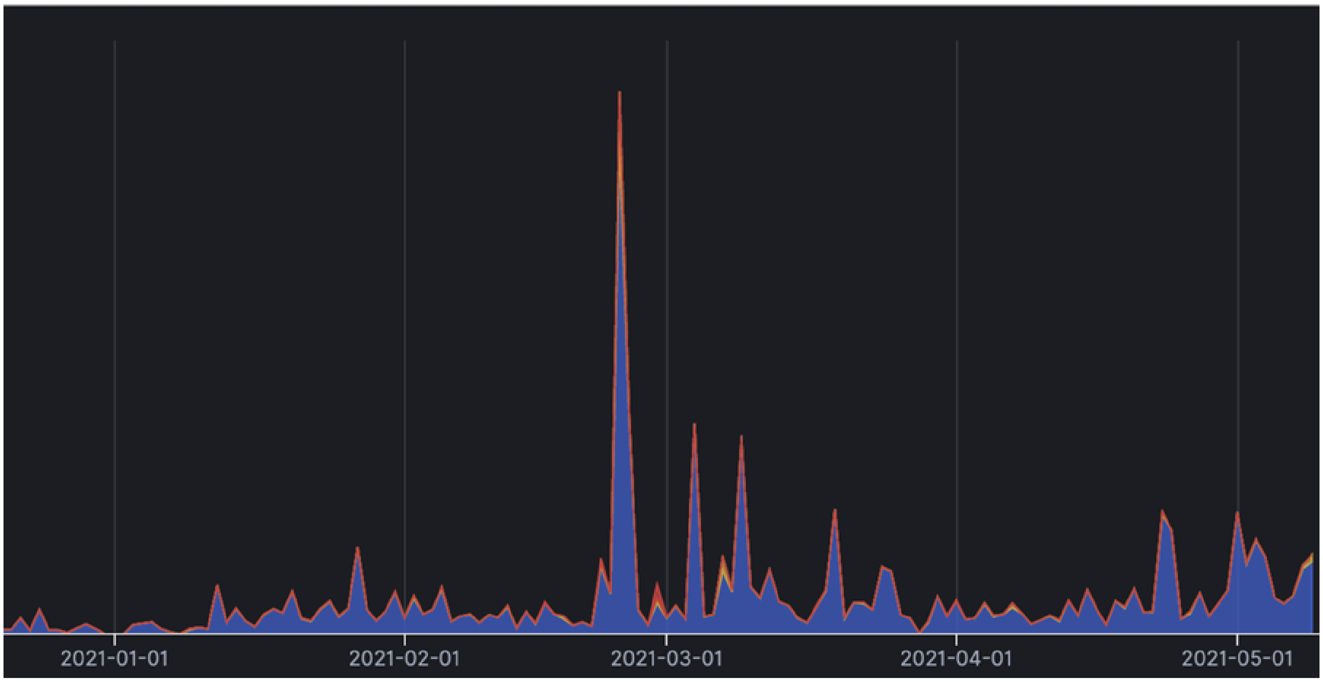


```

[CFG] Root Path................/vmfs/volumes/
[CFG] Key Size.................548 Bytes
[CFG] Public Key...............VALID
[CFG] Part Size................500mb
[CFG] Space Size...............0mb
[CFG] Min Size.................1mb
[CFG] Search Extension.........vmdk,vmem,vswp,log,vmsn
[CFG] New Extension............darkside
[CFG] Thread Count.............2
[CFG] ReadMe File..............darkside_readme.txt
[CFG] ReadMe Size..............1969 Bytes
[CFG] Landing URL#[01].........http://catsdegree.com/dbeeacbcdbca
[CFG] Landing URL#[02].........http://temisleyes.com/edbdeecdb
[CFG] User ID..................46017379a796803
[CFG] RC2 Key..................OK

[INF] Scanning: /vmfs/volumes/
```

Although the adversary recently claimed to vote for targets, the attacks are ongoing with packed and signed samples observed as recently as today (May 12, 2021):



Conclusion

Recently the Ransomware Task Force, a partnership McAfee is proud to be a part of, released a detailed paper on how ransomware attacks are occurring and how countermeasures should be taken. As many of us have published, presented on, and released research upon, **it is time to act.** Please follow the links included within this blog to apply the broader advice about applying available protection and detection in your environment against such attacks.

MITRE ATT&CK Techniques Leveraged by DarkSide:

Data Encrypted for Impact – T1486

Inhibit System Recovery – T1490

Valid Accounts – T1078

PowerShell – T1059.001

Service Execution – T1569.002

Account Manipulation – T1098

Dynamic-link Library Injection – T1055.001

Account Discovery – T1087

Bypass User Access Control – T1548.002

File Permissions Modification – T1222

System Information Discovery – T1082

Process Discovery – T1057

Screen Capture – T1113

Compile After Delivery – T1027.004

Credentials in Registry – T1552.002

Obfuscated Files or Information – T1027

Shared Modules – T1129

Windows Management Instrumentation – T1047

Exploit Public-Facing Application – T1190

Phishing – T1566

External Remote Services – T1133

Multi-hop Proxy – T1090.003

Exploitation for Privilege Escalation – T1068

Application Layer Protocol – T1071

Bypass User Account Control – T1548.002

Commonly Used Port – T1043

Compile After Delivery – T1500

Credentials from Password Stores – T1555

Credentials from Web Browsers – T1555.003

Credentials in Registry – T1214

Deobfuscate/Decode Files or Information – T1140

Disable or Modify Tools – T1562.001

Domain Account – T1087.002

Domain Groups – T1069.002

Domain Trust Discovery – T1482

Exfiltration Over Alternative Protocol – T1048

Exfiltration to Cloud Storage – T1567.002

File and Directory Discovery – T1083

Gather Victim Network Information – T1590

Ingress Tool Transfer – T1105

Linux and Mac File and Directory Permissions Modification – T1222.002

Masquerading – T1036

Process Injection – T1055

Remote System Discovery – T1018

Scheduled Task/Job – T1053

Service Stop – T1489

System Network Configuration Discovery – T1016

System Services – T1569

Taint Shared Content – T1080

Unix Shell – T1059.004

Raj Samani VP, Chief Technical Officer EMEA
Raj Samani is Chief Scientist and Fellow for the Enterprise business. He has assisted multiple law enforcement agencies in cybercrime cases and is a special advisor to the European Cybercrime...