A defender’s view inside a DarkSide ransomware attack

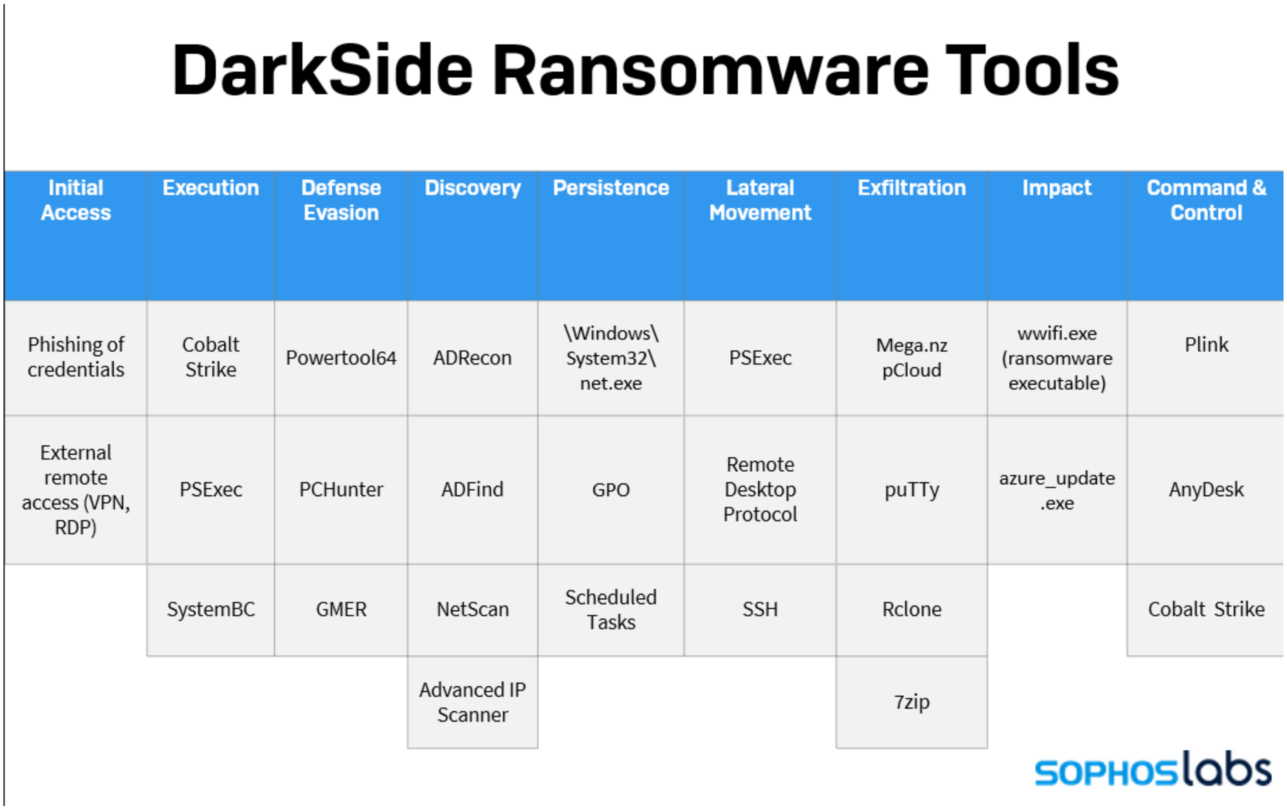
news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/

May 11, 2021

The recent ransomware intrusion of a major US gasoline pipeline operator was the work of an affiliate of DarkSide, a ransomware-as-a-service ring that has been responsible for at least 60 known cases of double-extortion so far this year. DarkSide has struck several high-profile victims recently, including companies listed on the NASDAQ stock exchange. But the disruption of Colonial Pipeline’s network led to the company shutting down its operational technology (OT) network as well—effectively cutting off a majority of the gasoline supply to the eastern United States.

Colonial Pipeline’s shutdown is not the first critical infrastructure issue triggered by a ransomware attack. Last February, a US-based natural gas facility was shut down for two days by a ransomware intrusion that spread to its OT network. And DarkSide has not avoided these types of companies, either, hitting a Brazilian energy company earlier this year. But the Colonial incident has potentially greater real-world impact—and has apparently made DarkSide’s operators more notorious than they’re comfortable with.

The Sophos Rapid Response team has been called in for incident response or to intervene during an attack involving DarkSide on at least five different instances in the past year.



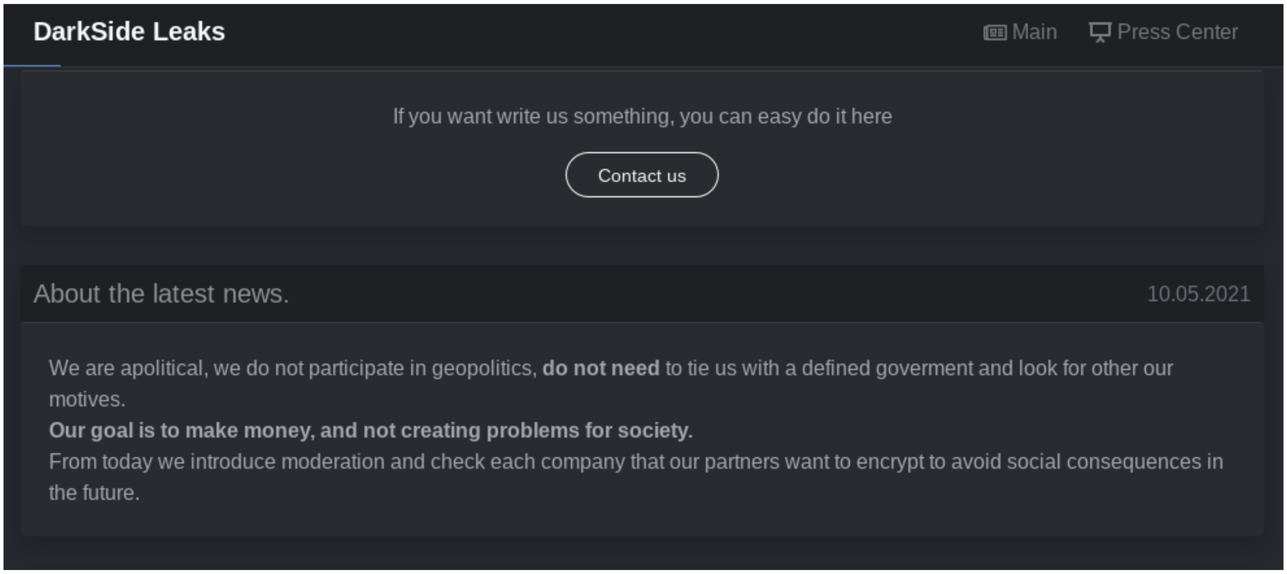
DarkSide Ransomware Tools

Initial Access	Execution	Defense Evasion	Discovery	Persistence	Lateral Movement	Exfiltration	Impact	Command & Control
Phishing of credentials	Cobalt Strike	Powertool64	ADRecon	\Windows\System32\net.exe	PSExec	Mega.nz pCloud	wwifi.exe (ransomware executable)	Plink
External remote access (VPN, RDP)	PSExec	PCHunter	ADFind	GPO	Remote Desktop Protocol	puTTy	azure_update.exe	AnyDesk
	SystemBC	GMER	NetScan	Scheduled Tasks	SSH	Rclone		Cobalt Strike
			Advanced IP Scanner			7zip		

Coming over to DarkSide

DarkSide emerged last summer, gaining notice with its purported “honor among thieves” approach: the gang claimed to have a code of conduct that forbid targeting industries and non-profit organizations connected to the public interest.

The ring has struggled to keep its “honorable” reputation, using their leak site as a platform to counter bad news. When ransomware recovery company Coveware warned that DarkSide’s use of Iranian hosting posed potential peril of sanctions violations if companies paid them, DarkSide’s operators posted a “press release” denying they used any Iranian IT services. The Colonial Pipeline attack again has the DarkSide gang backpedaling, pleading in a post on their web page that they are “apolitical” and that their goal is “to make money, and not creating problems for society.”



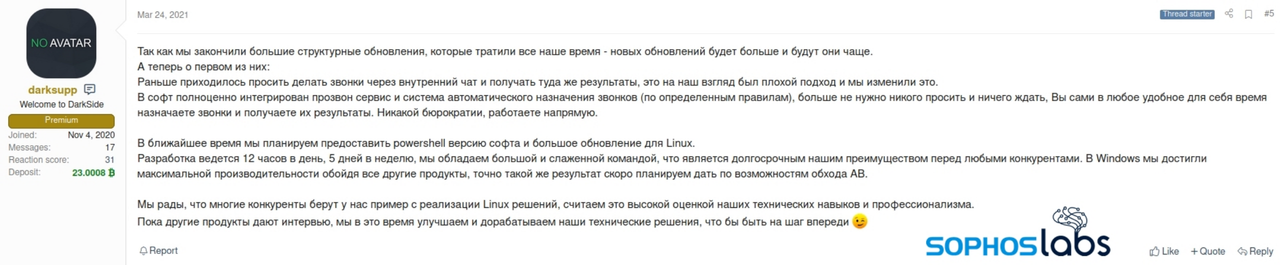
If you want write us something, you can easy do it here

About the latest news. 10.05.2021

We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined goverment and look for other our motives.
Our goal is to make money, and not creating problems for society.
From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.

The ransomware threat actors claim their actions are ‘apolitical’

The gang previously promised to spare healthcare organizations, as well as others involved in vaccine distribution, because of the negative attention such attacks could potentially bring from within the gang’s home country. Because of the way DarkSide operates, it’s not clear how much control the keepers of the DarkSide brand have over the affiliates who do the actual work of breaking into networks and launching their ransomware.



Joined: Nov 4, 2020
Messages: 17
Reaction score: 31
Deposit: 23.0008 ₿

Mar 24, 2021

Так как мы закончили большие структурные обновления, которые тратили все наше время - новых обновлений будет больше и будут они чаще.
А теперь о первом из них:
Раньше приходилось просить делать звонки через внутренний чат и получать туда же результаты, это на наш взгляд был плохой подход и мы изменили это.
В софт полноценно интегрирован прозвон сервис и система автоматического назначения звонков (по определенным правилам), больше не нужно никого просить и ничего ждать, Вы сами в любое удобное для себя время назначаете звонки и получаете их результаты. Никакой бюрократии, работаете напрямую.

В ближайшее время мы планируем предоставить powershell версию софта и большое обновление для Linux.
Разработка ведется 12 часов в день, 5 дней в неделю, мы обладаем большой и слаженной командой, что является долгосрочным нашим преимуществом перед любыми конкурентами. В Windows мы достигли максимальной производительности обойдя все другие продукты, точно такой же результат скоро планируем дать по возможностям обхода АВ.

Мы рады, что многие конкуренты берут у нас пример с реализации Linux решений, считаем это высокой оценкой наших технических навыков и профессионализма.
Пока другие продукты дают интервью, мы в это время улучшаем и дорабатываем наши технические решения, что бы быть на шаг впереди 😉

DarkSide’s affiliate ad: “Who are we looking for? A limited number of stable and adequate partners who understand why it is necessary to upload data, what is backups and how to delete them, Russian-speaking, with payouts from 500k.”

DarkSide follows in the footsteps of double-extortion ransomware operators such as REvil, Maze, and LockBit—exfiltrating business data before encrypting it, and threatening public release if the victims don’t pay for a decryption key. Like those other targeted operations, DarkSide makes hefty ransom demands. In one case Sophos Rapid Response worked on last year, the ring demanded $4 million (which went unpaid).

Beyond the business model, DarkSide follows generally the same tactics, techniques, and procedures of many other targeted ransomware campaigns — a mix of native Windows features, commodity malware (including SystemBC), and off-the-shelf system and exploit tools (including Cobalt Strike). This is in part because of DarkSide’s affiliate model.

The creators of DarkSide outsource the initial compromise of targets and deployment of DarkSide’s cryptographic ransomware to network penetration specialists, who hand off ransom victim “customer service” to DarkSide’s core operators. Those affiliates likely have prior experience playing the same role for other ransomware syndicates.

In Sophos' experience in data forensics and incident response to DarkSide attacks, the initial access to the target's network came primarily as a result of phished credentials. This is not the only way ransomware attackers can gain a foothold but it seems to be prevalent in cases involving this type of ransomware, possibly as a result of the affiliates' preferences.

Unlike some other ransomware players, DarkSide is capable of encrypting Linux computers as well as those running Windows, which makes it a more desirable tool for threat actors who want to target large enterprises.

While some recent targeted ransomware operations from other gangs have sprung quickly, launching their attack within days, the actors behind DarkSide campaigns may spend weeks-to-months poking around inside an organization's network before activating their ransomware payload.

Dwell Time

Metric	Dwell Time (Days)
Minimum	44
Median	45
Maximum	88

Over the course of that dwell time, the intruders exfiltrate as much data as possible. Darkside's ransom notes claim the theft of large amounts of data, often from several departments within an organization, such as Accounting and R&D. Using PSExec, Remote Desktop connections, and (in the case of Linux servers) SSH to move laterally within the network, the DarkSide actors uploaded archives of stolen files to the cloud storage providers Mega or pCloud in cases we've investigated.

File system activity

The DarkSide ransomware performs specific steps to encrypt a document, first appending a unique file extension to the name of every targeted document type before encrypting the file.

The malware checks whether the Windows 10 user account under which it is running has administrative privileges; If it does not, the malware attempts to elevate its privileges using the CMSTPLUA technique.

DarkSide retrieves the target computer's network adapter MAC address, and then computes CRC32 five times on the first six bytes of the adapters' MAC address, where the initial seed is 0xDEADBEEF. Because the first six bytes of a MAC address are registered to manufacturers, many of the affected corporate machines would end up with the same file extension appended to documents simply as a result of the machines being part of a bulk purchase.

The attackers (likely the same affiliates involved in the initial access) also make an effort to terminate software that, if it was running, might otherwise interfere with the encryption process. We've observed them terminate the services relating to enterprise backup software from Commvault and Veeam, shut down the mail server software MailEnable, and kill SQL server database services, so they can encrypt any database they find. They also attempt to uninstall or tamper with Sophos services if they're present on the machine. Like other ransomware, DarkSide also deletes Volume Shadow Copies, which could help recover some of the encrypted data if left unmolested.

Encrypting every document file type on a hard drive takes time, and if the process gets interrupted mid-way through, some of the unencrypted files could be recovered easily. Renaming the file with a new extension before encrypting it gives an attacker the ability to make it appear as though everything has been encrypted, as the file extension change cuts the ties between the document file type and its associated application.

The encryption process for DarkSide always has followed these steps:

Step	Operation	Purpose
1	CreateFile (Generic Read/Write)	Open original document for reading and writing.
2	ReadFile	Read last 144 bytes of original document (look for decryption blob).
3	CloseFile	Close original document (no changes made).
4	CreateFile (Read Attributes)	Open original document.
5	SetRenameInformationFile	Rename document by adding a specific file type extension, for example .c0d2f38a
6	CloseFile	Close now renamed document.
7	CreateFile (Generic Read/Write)	Open renamed original document.
8	ReadFile	Read renamed original document.
9	WriteFile	Write encrypted document in renamed original document.
10	WriteFile	Add decryption blob, 144 bytes, to end of file.

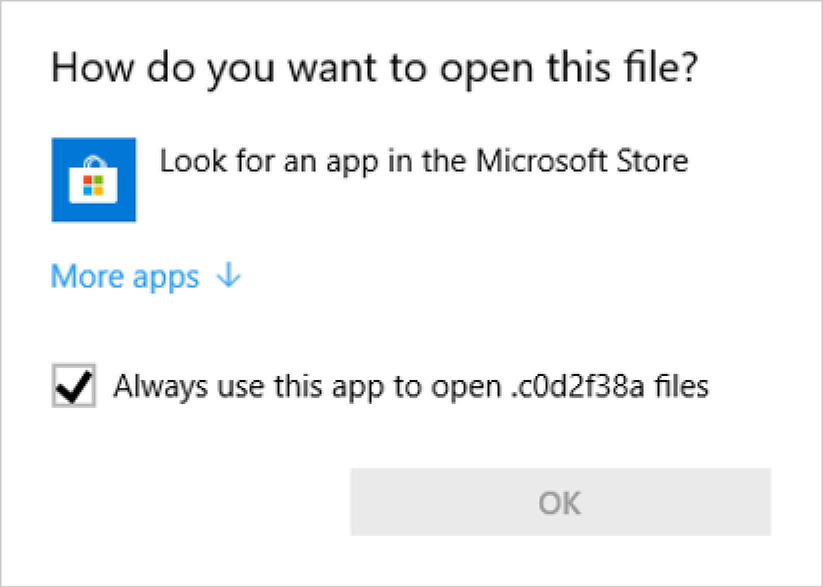
11	CloseFile	Close renamed, now encrypted, document.

Solving the ugly icon problem

There are several benefits to the threat actors when ransomware appends a new or unusual file extension to the files it encrypts. Of course, it decouples the encrypted documents from their normally associated applications, which means the user can't interact with them in the usual way (by double-clicking). The unusual file suffixes represent both a signal to the ransomware that a file has already been encrypted (so the ransomware engine doesn't re-encrypt or double-encrypt the same files), and carry a side benefit: it prevents other ransomware (at least, the families that target the documents they will attack using hardcoded lists of file suffixes—a lot of them) from encrypting those same files.

One downside to switching the file suffix is that, when it loses its association with its application, the document no longer uses the icon tied to that association. So an encrypted Word document, for instance, just has a blank icon rather than a pretty picture of a document with a *W* on it.

DarkSide appears to be very concerned with this problem of the poor appearance of encrypted hard drives, so they have worked out a solution.



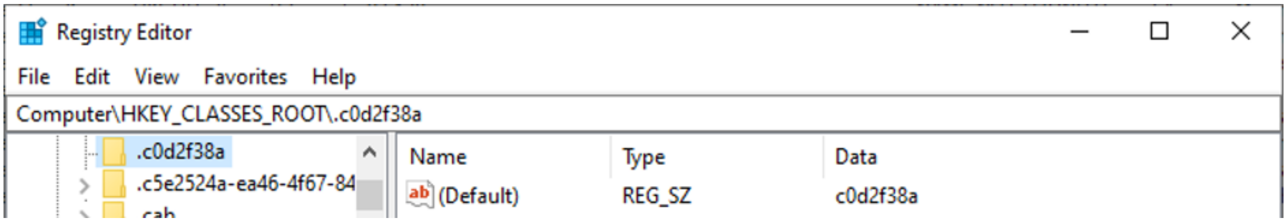
How do you want to open this file?

Look for an app in the Microsoft Store

☑ Always use this app to open .c0d2f38a files

Encrypted documents typically receive a new file extension and are consequently no longer associated with the document's productivity application

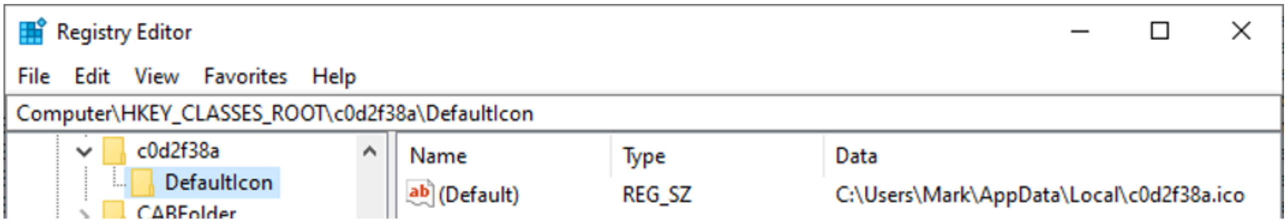
DarkSide drops an image file — an icon — into the **%APPDATA%\Local** directory, named after the same eight character extension the ransomware has used to rename every targeted file. In this example, that extension is **.c0d2f38a**. It then writes out a Windows Registry key in **HKEY_CLASSES_ROOT** that associates files with the unique and peculiar file extension it has generated to that icon file, so that encrypted files suddenly have a unique icon of their very own.



Computer\HKEY_CLASSES_ROOT\.c0d2f38a

Name	Type	Data
(Default)	REG_SZ	c0d2f38a

Registering the ransomware file type extension …



Computer\HKEY_CLASSES_ROOT\c0d2f38a\DefaultIcon

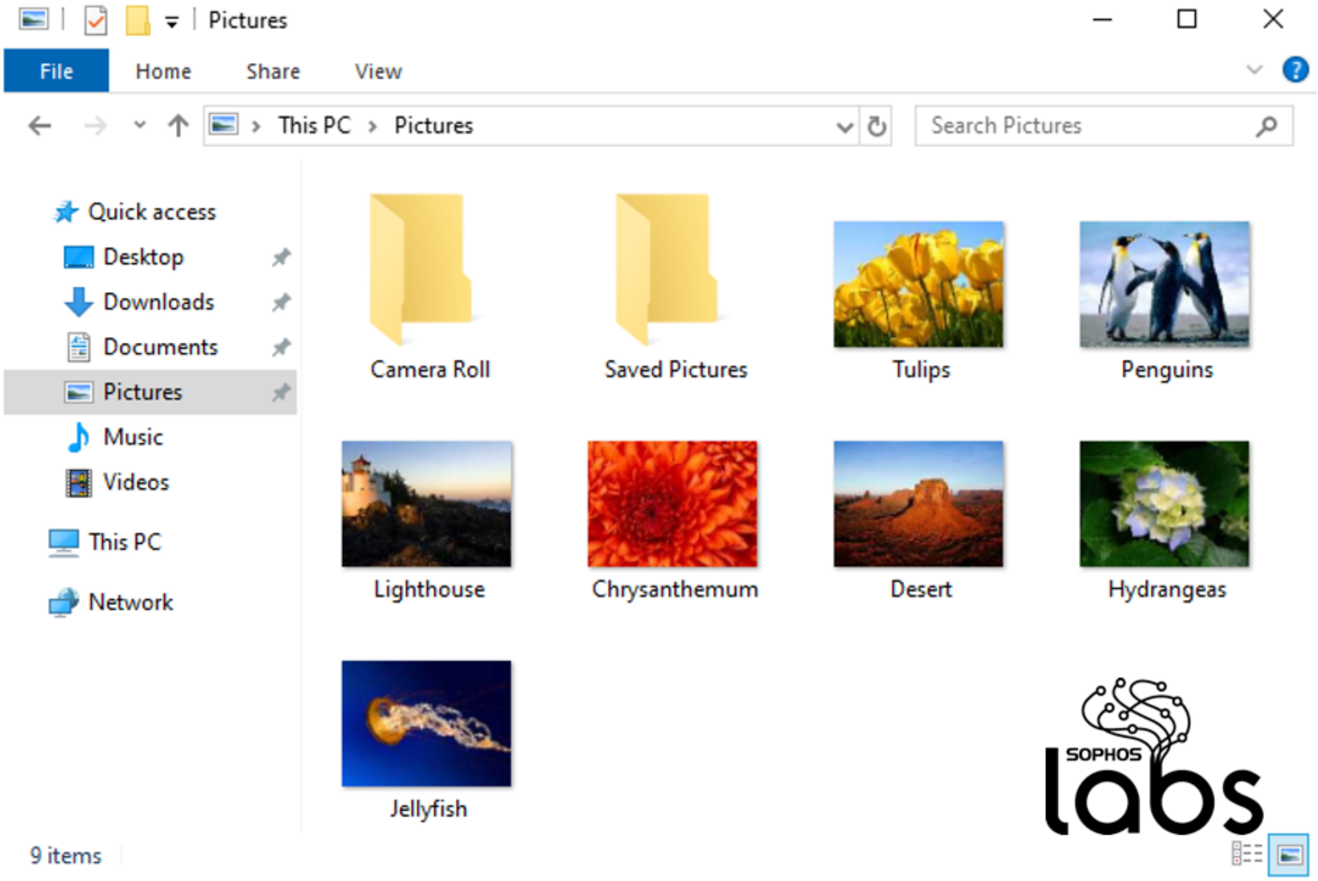
Name	Type	Data
(Default)	REG_SZ	C:\Users\Mark\AppData\Local\c0d2f38a.ico

…

and referencing it to the icon file

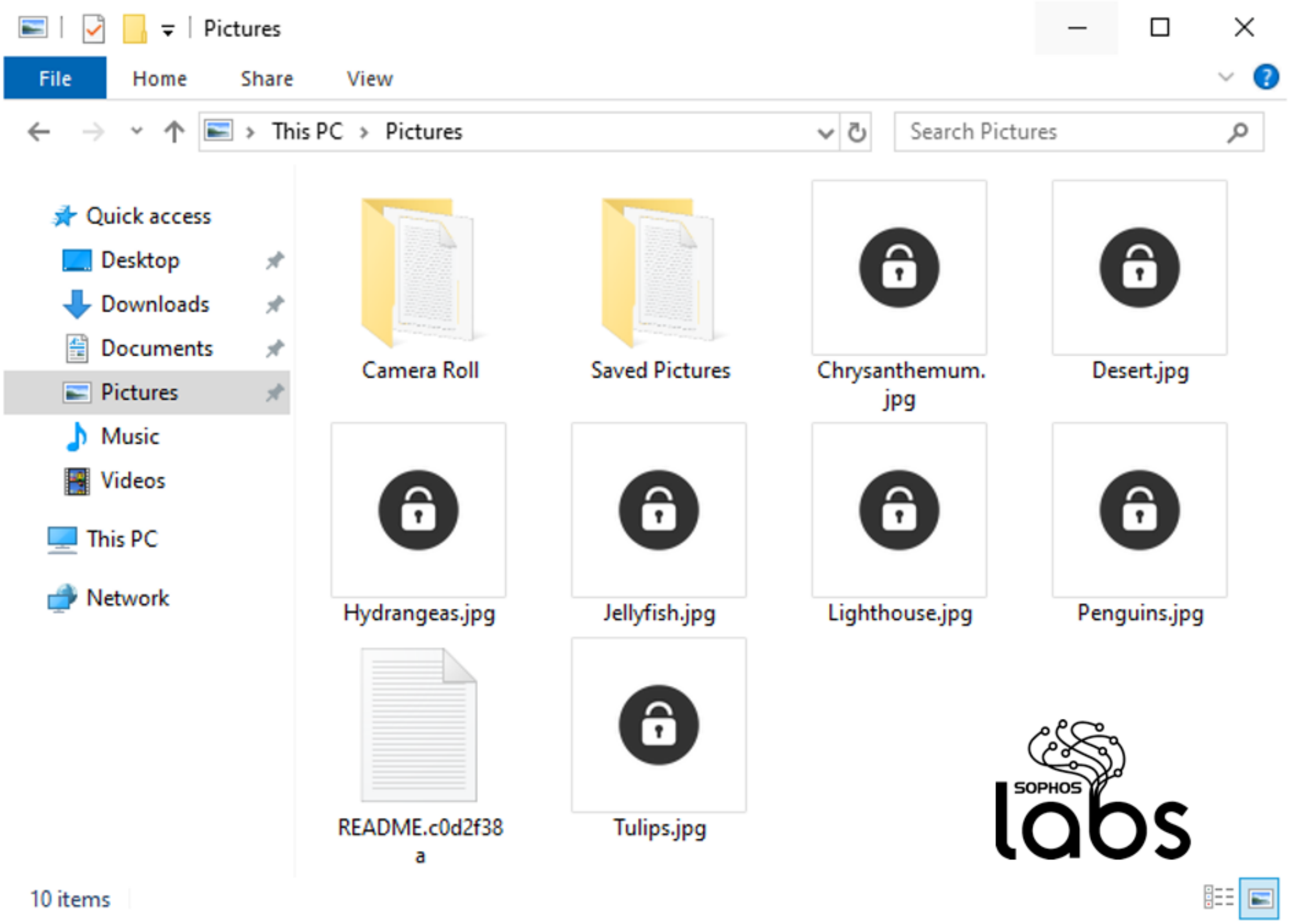
DarkSide's .ico file is so thorough that it contains several icon sizes, so your computer will display the appropriately sized icon according to your preferences. It comes in 64×64, 32×32, 24×24, and 16×16 pixels, and it looks like a black padlock.

So what happens is that a folder full of documents goes from looking like this:



Pictures not yet attacked by DarkSide ransomware.

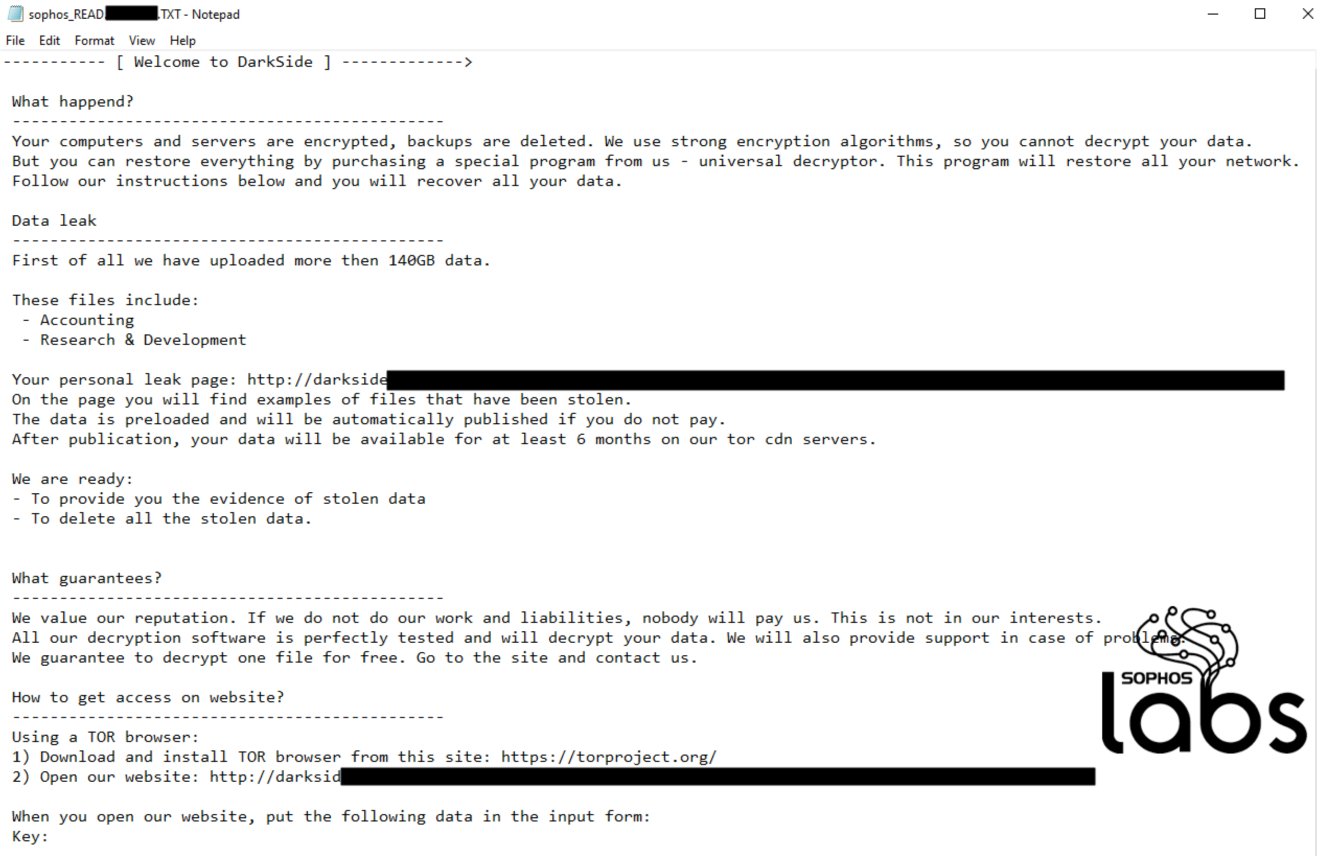
…to looking like a folder full of “locked” files, like this:



Pictures encrypted by DarkSide with the lock icon.

After the encryption is complete

After the ransomware has concluded the file encryption, it drops this ransom note in each folder that contains the newly scrambled files:

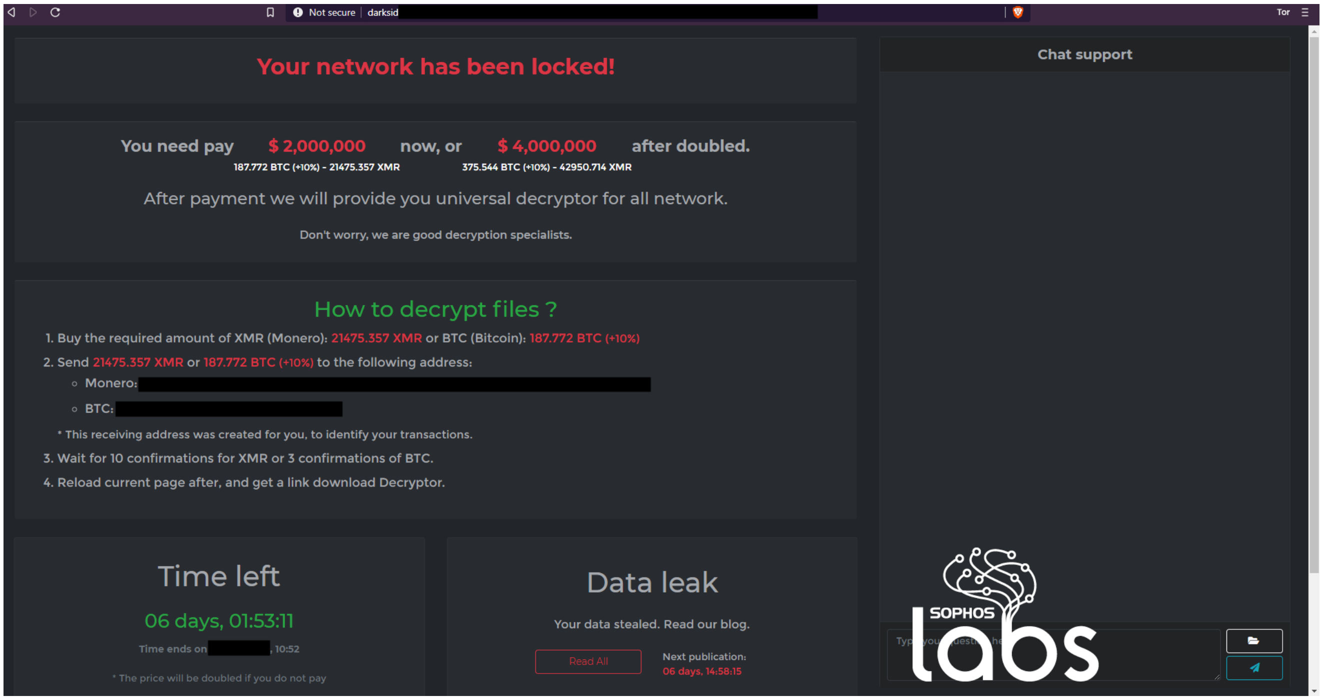


sophos_READ[redacted].TXT - Notepad

```
----------- [ Welcome to DarkSide ] ------------->

 What happend?
 ----------------------------------------------
 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 uploaded more then 140GB data.

 These files include:
  - Accounting
  - Research & Development

 Your personal leak page: http://darkside[redacted]
 On the page you will find examples of files that have been stolen.
 The data is preloaded and will be automatically published if you do not pay.
 After publication, your data will be available for at least 6 months on our tor cdn servers.

 We are ready:
 - To provide you the evidence of stolen data
 - To delete all the stolen data.


 What guarantees?
 ----------------------------------------------
 We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
 All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
 We guarantee to decrypt one file for free. Go to the site and contact us.

 How to get access on website?
 ----------------------------------------------
 Using a TOR browser:
 1) Download and install TOR browser from this site: https://torproject.org/
 2) Open our website: http://darksid[redacted]

 When you open our website, put the following data in the input form:
 Key:
```

The ransom note, redacted.

The link takes the victim to the payment page, hosted on the dark web:



Your network has been locked!

You need pay $ 2,000,000 now, or $ 4,000,000 after doubled.
187.772 BTC (+10%) - 21475.357 XMR | 375.544 BTC (+10%) - 42950.714 XMR

After payment we will provide you universal decryptor for all network.

Don't worry, we are good decryption specialists.

How to decrypt files ?

1. Buy the required amount of XMR (Monero): 21475.357 XMR or BTC (Bitcoin): 187.772 BTC (+10%)
2. Send 21475.357 XMR or 187.772 BTC (+10%) to the following address:
   - Monero: [redacted]
   - BTC: [redacted]

   * This receiving address was created for you, to identify your transactions.
3. Wait for 10 confirmations for XMR or 3 confirmations of BTC.
4. Reload current page after, and get a link download Decryptor.

Time left

06 days, 01:53:11

Time ends on [redacted], 10:52

* The price will be doubled if you do not pay

Data leak

Your data stealed. Read our blog.

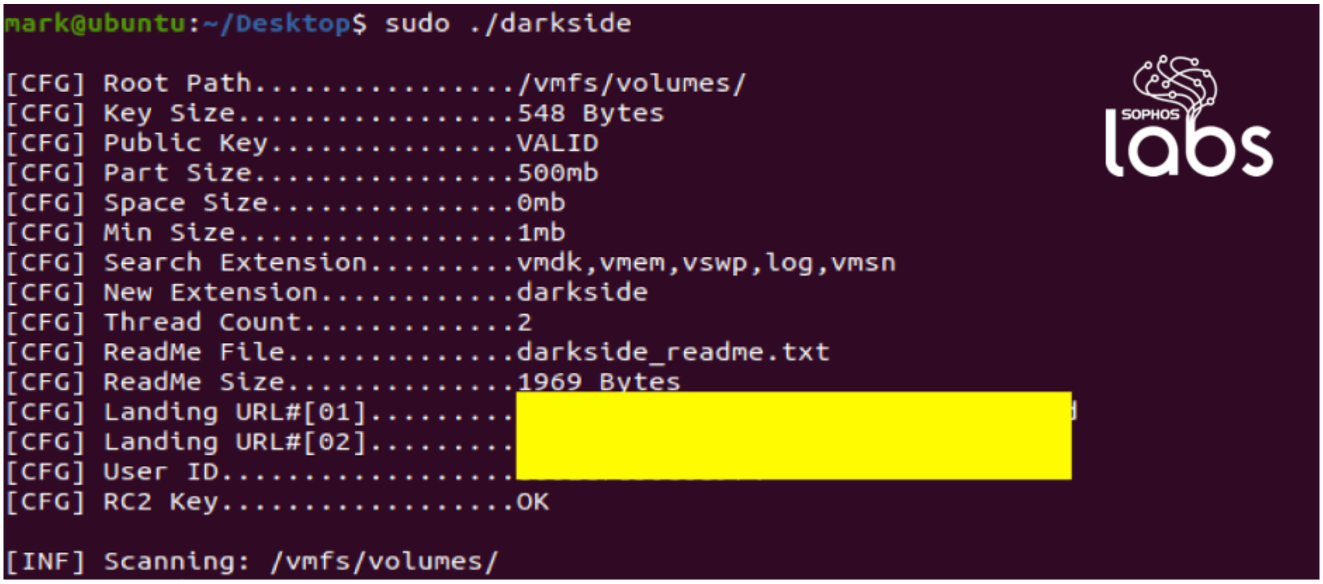
Next publication:
06 days, 14:58:15

The ransom demand gives the target a handy conversion of the ransom demand into both Bitcoin and Monero (Dogecoin not currently accepted for payment), a countdown lock to when the ransom demand doubles, and a link to the page that hosts examples of “Your data stealed.”

Attacking Linux, encrypting VMDK files

The DarkSide ransomware adversary not only attacks Windows machines, but also deploys ELF binaries (Executable and Link Format) to attack data on Linux machines. The Linux version of the DarkSide ransomware specifically targets VMDK files, which are virtual hard disk drives to be used in virtual machines like VMware and VirtualBox.

Console output of the Linux version reveals this ransomware is specifically searching for file extensions associated with virtual hard disk drives on Linux, including on hypervisor operating systems like VMWare's ESX, where the virtual hard drives for virtual machines are stored under the /vmfs/volumes/ file path:



```
mark@ubuntu:~/Desktop$ sudo ./darkside

[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]........ [redacted]
[CFG] Landing URL#[02]........
[CFG] User ID.................
[CFG] RC2 Key..................OK

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

Turning away from the DarkSide

Sophos defends against DarkSide in multiple ways. There are behavioral and dynamic protections, which include the CryptoGuard feature in Intercept X, and both conventional endpoint detections for Windows (**Troj/Ransom-GAZ, Troj/PShl-E, VBS/Agent-BGYV**) and Linux (**Linux/Ransm-J**) malicious executables, and next-gen detections for in-memory functions (**Mem/DarkSide-A, HPmal/DarkS-A**) and behaviors (**AMSI/Inject-H, AMSI/PSRans-A, ML/PE-A**) on Windows.

Acknowledgments

SophosLabs would like to acknowledge Yusuf Arslan Polat, Gabor Szappanos, Suriya Natarajan, Szabolcs Lévai, and Ferenc László Nagy for their contributions to this post.