## Today's Ransomware – Darkside

Nov 2, 2020

1. Blocked by trueEP®

💡 trueEP Ent 2. 0		- 🗆 ×									
â <sup>≗</sup>											
ि हिल	타입 날짜 랜성웨 2020-11-02 12:03:46	프로세스 파일이름 darkside,exe Behavior Blocking									
🏹 스마트 백업											
을 검사 제외											
		<u>찾기</u> 1000개 더 복원 삭제									
<b>ଡି</b> ଅଖାରା =	날짜	파일이름									
<b>())</b> 설정											
(?) 도움말											

2. Victim in case trueEP<sup>®</sup> was not installed - All file name's extensions were changed to Random Extension.

📙 🗹 📕 🚽 🖓	새 폴더				- 🗆	×				
파일 홈 ·	공유	보기				~ 🧃				
$\leftarrow \rightarrow \cdot \uparrow$	→ · ↑ · · · · · · · · · · · · · · · · ·									
🖈 바로 가기		이름	수정한 날짜	유형	크기					
💭 바탕 화면	*	README.c3aa5e55	2020-11-02 오전	텍스트 문서	3KB					
		📄 문서1.docx.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	16KB					
↓ 다운로드	A	📄 문서2.docx.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	16KB					
🏥 문서	1	📄 문서3.docx.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	16KB					
📰 사진	*	📄 문서4.xlsx.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	18KB					
📕 동영상		📄 문서5.pptx.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	5,526KB					
 ▶ 음악		📄 문서6.pdf.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	128KB					
• • •		📄 문서7.txt.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	1KB					
less one Drive		🗋 압축.zip.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	3,488KB					
💻 내 PC		📄 압축2.zip.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	7,687KB					
<u> </u>		이미지.bmp.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	159KB					
💣 네트워크		이미지.JPG.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	282KB					
		이미지.png.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	23KB					
		이미지.psd.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	396KB					
		 이미지2.jpg.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	195KB					
		0□ ⊼ 3.jpg.c3aa5e55	2020-11-02 오전	C3AA5E55 파일	198KB					
16개 항목										

## 3. Screen of Victim

I README.c3aa5e55 - Windows 메모장	_		×							
파일(F) 편집(E) 서식(O) 보기(V) 도움말										
[ Welcome to Dark ]	>					^				
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 100 GB data.										
Example of data: - Accounting data - Executive data - Sales data - Customer Support data										
- Marketing data						~				
	Ln 1, Col 1	100%	Windows (CRLF)	UTF-	8					

0												
휴지통	문서7txte	NEADME.cBaa 5e55										
문서비 doex	압축 zip.c3											
문서[2.doex	압축2.ap.c											
문서3 pdf.c	새 줄데											
	e											
문서4.xlax	Microsoft Edge											
문서5 pptx	LOG.cBash											
문서6.pdf.c	darkside											
م #	검색하려	면 여기에 입력하십	시오.	囯	е		<b>∻</b>		~	、 [囗 🗤 A	오전 11:49 2020-11-02	5