Today's Ransomware – Nemty1.6

Oct. 11, 2019

## 1. Blocked by true $\ensuremath{\mathsf{P}}^{\ensuremath{\mathbb{R}}}$

Image: strue EP Monitor 2. 0. 19. 927 X										
Home Home										
	Туре	Date	Process	File Name	Size					
Defense Defense		2019-10-10 17:29:17	Nemty1.6	Behavior Blocki	0					
Smart Backup										
Exclusion										
	Backup Log	Find		0 Restore	Delete					
J	Date	F	File Name		Size					
🕢 Update										
<b>(်)</b> Set										
Help										
				147						

2. Victim in case trueEP<sup>®</sup> was not installed - All file name's extensions ware changed to \_NEMTY\_random\_.

📙   🛃 📙 🖵   A	세 폴더				- 🗆	×
파일 홈 중	공유	보기				~ 🕐
← → ✓ ▲ → 새 풀더 ↓ 새 풀더 검색					Ą	
		이름	수정한 날짜	유형	크기	
★ 즐겨찾기		_NEMTY_XM859THDECRYPT	2019-10-11 오전	텍스트 문서	4KB	
바탕 화면	A	📄 문서1.docxNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	17KB	
↓ 다운로드	*	📄 문서2.docxNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	17KB	
🔮 문서	*	📄 문서3.docxNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	17KB	
📰 사진	*	📄 문서4.xlsxNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	18KB	
🚪 동영상		📄 문서5.pptxNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	5,526KB	
🎝 음악		📄 문서6.pdfNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	128KB	
		📄 문서7.txtNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	1KB	
OneDrive		📄 압축.zipNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	3,488KB	
🛄 내 PC		📄 압축2.zipNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	7,687KB	
		이미지.bmpNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	159KB	
💣 네트워크		이미지.JPGNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	283KB	
		이미지.pngNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	23KB	
		이미지.psdNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	397KB	
		이미지2.jpgNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	195KB	
		이미지3.jpgNEMTY_XM859TH_	2019-10-11 오전	_NEMTY_XM85	198KB	
16개 항목						

## 3. Screen of Victim

 $\times$ 파일(F) 편집(E) 서식(O) 보기(V) 도움말(H) NEMTY PROJECT V1.6 Don't worry, all your encrypted files can be restored. It's a business, if we can't provide full decryption, other people won't trust us. In confirmation, that we have decryption key, we can provide you test decryption. On our website you can upload 1 encrypted picture (png,bmp,jpg,gif) and get it decrypted. There is no way to decrypt your files without our help. Don't trust anyone. Even your dog. There is 1 way how to get to the website: 1) Any browser a) Open your browser b) Type this url: nemty.hk/pay c) Upload this note NEMTY DECRYPTION KEY: NH67db9HGLC0u4F1nKjuBU1PKMsO3P2ovhxGpd0Y7ImQbOa+JMMXY+3pDj1qC1a+MoKSUZUB5yL0PSdhWCVl2cm6cmtr5C0a4F1nKjuBU1PKMsO3P2ovhxGpd0Y7ImQbOa+JMMXY+3pDj1qC1a+MoKSUZUB5yL0PSdhWCVl2cm6cmtr5C0a4F1nKjuBU1PKMsO3P2ovhxGpd0Y7ImQbOa+JMMXY+3pDj1qC1a+MoKSUZUB5yL0PSdhWCVl2cm6cmtr5C0a4F1nKjuBU1PKMsO3P2ovhxGpd0Y7ImQbOa+JMMXY+3pDj1qC1a+MoKSUZUB5yL0PSdhWCVl2cm6cmtr5C0a4F1nKjuBU1PKMsO3P2ovhxGpd0Y7ImQbOa+JMMXY+3pDj1qC1a+MoKSUZUB5yL0PSdhWCVl2cm6cmtr5C0a4F1nKjuBU1PKMsO3P2ovhxGpd0Y7ImQbOa+JMMXY+3pDj1qC1a+MoKSUZUB5yL0PSdhWCVl2cm6cmtr5C0a4F1nKjuBU1PKMsO3P2ovhxGpd0Y7ImQbOa+JMMXY+3pDj1qC1a+MoKSUZUB5yL0PSdhWCVl2cm6cmtr5C0a4F1nKjuBU1PKMsO4F1nKjuBU1PKmsO4F1nKjuBU1PKmsO4F1nKjuBU1PKmsO4F1nKjuBU1PKmsO4F1nKjuBU1PKmsO4F1nKjuBU1PKmsO4F1nKjuBU1PKmsO4F1nKjuBU1PKmsO4F1nKjuBU1PKmsO4F1nKjuBU1PKMsO4F1nKjuBU1PKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjuBKmsO4F1nKjt8A8gLV9sQWUilfaL0iTJKxTVrGyg36m4yLQvxlfapwoq5G49Z2OYtkxBVGJVwMhpBUN5KBN9YCKUiET8eT+wAN7qCm19fMawr 143eeO4H3E0I5zeIAw9IIZxtWEDTn3aSfPxOc2/D1cjazSB5K+0rKZENGrlzzLi/JpijOgLUbmDX5dmsPcOfGxluHorRiPVJIqTZ1ex/Wg 후지통 문서4 xlsx NEMTY\_XM8 문서5.pptx 9TH\_-DECR VPT 7 문서6.pdf.

