

# Anatomia e një Sulmi Kripto-Ransomware



Variantet e reja të ransomware-ve të njohura si CryptoLocker, CryptoDefense dhe CryptoWall po përhapen me shpejtësi përmes emaileve keqdashës, shkarkimeve nga kompjuteri ose përmes malware-ve të ndryshëm. Pasi të jeni infektuar, kripto-ransomware infekton të gjithë skedarët tuaj, i enkripton ata në mënyrë të pathyeshme dhe kërkon një shpërblim prej 300\$-500\$ në Bitcoin për t'i dekriptuar ato.

## 5 FAZAT E KRIPTO-RANSOMWARE

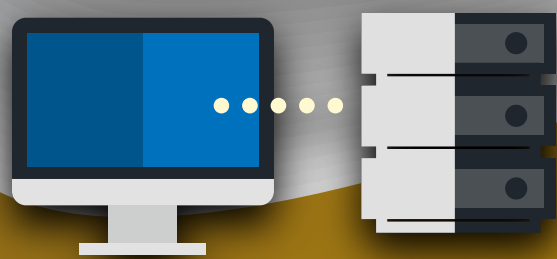
### 1 INSTALIMI

Pasi kompjuteri i viktimës infektohet, kripto-ransomware instalon çelësa në Regjistrin e Windows, të cilët aktivizohen automatikisht sa herë që kompjuteri ndizet.



### KOMUNIKIMI ME SERVERIN

### 2



Përpara se kripto-ransomware të mund të veprojë, ai komunikon me një server të menaxhuar nga sulmuesi që e zotëron atë.

### 3 ÇELËSAT KRIPTOGRAFIKË

Pasi ransomware dhe serveri identifikojnë njëri-tjetrin, serveri gjeneron dy çelësa kriptografikë. Një çelës ruhet në kompjuterin e viktimës dhe çelësi i dytë ruhet në mënyrë të sigurt në serverin e sulmuesve.



### ENKRIPTIMI

### 4

Me gjenerimin e çelësve kriptografikë, ransomware fillon të enkriptojë çdo skedar, duke nisur që nga dokumentet e Microsoft Office tek imazhet .jpg, etj..

### 5 ZHVATJA E PARAVE

Ransomware shfaq në ekranin e viktimës një afat kohor për të paguar, para se kriminelët të shkatërrojnë çelësin që dekripton skedarët. Pagesa zakonisht varion nga 300\$-500\$, e cila duhet të paguhet në Bitcoin ose mënyra të tjera elektronike.



## QËNRONI TË SIGURT



#### KUFIZONI "WRITE PERMISSIONS"

në serverat e skedarëve sa më shumë të jetë e mundur



#### PËRDORNI MBROJTJEN E AVANCUAR ENDPOINT

kjo mund të identifikojë variante të reja malware dhe të zbulojë trafikun keqdashës



#### PËRDORNI MBROJTJE PËR WEBIN DHE EMAILIN

për të bllokuar hyrjen në faqet e internetit keqdashëse dhe për të skanuar të gjitha shkarkimet që kryeni në kompjuterin tuaj



**EDUKONI PËRDORUESIT** të kontaktojnë qëndën e IT nëse hasin dritare pop-up të dyshimta



**KRYENI RREGULLISHT BACK UP PËR SKEDARËT TUAJ;** testojini ato për t'u siguruar që të dhënat mund të rikthehen në mënyrë të sigurt