2017

Alt hvad du behøver at vide om Ransomware

Kim Kulebjerg

NewTech IT

01-01-2017

Indholdsfortegnelse

Alt hvad du behøver at vide om Ransomware 2
Hvad er Ransomware og hvad gør det? 2
Lidt baggrund 2
Måder Ransomware inficere din computer på. (leveringsmetoder) 2
Populære Ransomware varianter (infektions metoder) 3
Sådan fungerer det 4
Hvordan du beskytter din Computer imod Ransomware 4

Alt hvad du behøver at vide om Ransomware

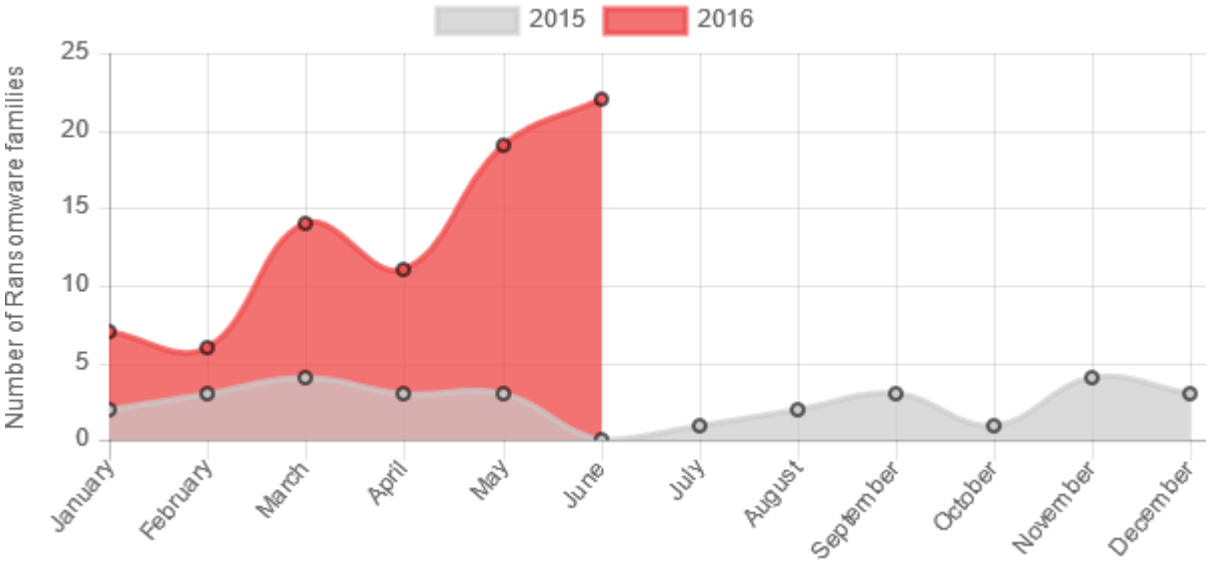
Malware angreb vokser mere og mere og bliver mere sofistikerede for hver dag der går. I en af vores tidligere guider gennemgik vi de forskellige typer af malware, deres infektion mekanismer og hvordan de fungerer inden for et system. Der er i øjeblikket, én kategori af malware, der bliver stadig mere populært og kaldes "ransomware." I denne guide, vil vi diskutere hvad ransomware er og hvilke strategier og teknikker, der anvendes i at skabe og udbrede denne seneste tendens i internet-kriminalitet

Hvad er Ransomware og hvad gør det?

Ransomware er en kategori af malware, der deaktiverer computerens funktionalitet ved at begrænse din adgang til computeren, filer og/eller mapper. Derefter, kræves en løsesum som du skal betales til malware forfatter for at genskabe systemets funktionalitet. Programmet ransomware låser normalt en computer og viser forskellige billeder fra offentlige myndigheder for at skræmme og afpresse penge fra dig. Ud over låse dig ude af din computer, vil nogle ransomware kryptere og skjule dine personlige filer, så du ikke har adgang til dem længere

Lidt baggrund

Ransomware er ikke et nyt fænomen. Den første forekomst af ransomware udkom tilbage i 1989, som blev kendt som PC Cyborg Trojan (også kendt som Aids Info Disk (AIDS)). Den berygtede Trojan erstattet autoexec.bat fil på den inficerede computer og talte hvor mange gange en computer havde startet. Når systemet havde startet/genstartet 90 gange, ville en trojansk hest skjule mapper og ændre alle filnavne på drev C:\, og dermed gøre systemet ubrugeligt. For at genskabe systemets funktionalitet, forlangte hackeren, at brugeren betalte $189 til "PC Cyborg Corporation." Selvom ransomware fænomenet ikke er nyt, er det steget drastisk siden 2005. Ransomware angreb blev først populære i Rusland, men i de sidste par år, er antallet af ransomware angreb steget på verdensplan. Trend Micro har anslået at alene i første halvår af 2016 er malware angreb steget med 172% i forhold til 2015.



Måder Ransomware inficere din computer på. (leveringsmetoder)

Ransomware kan inficere din computer på samme måde som de fleste andre malware. Nogle af de mest almindelige måder hvorpå en computer kan blive inficeret med ransomware er:

- **Drive-by download**: Dette er den mest almindelige måde at inficere din computer med ransomware. Alt hvad det kræver er at du besøger en skadelig eller kompromitteret hjemmeside, klikker på et ondsindet annonce/link, eller åbner en skadelig vedhæftet fil og din computer er inficeret

- **At udnytte dine programmers sårbarhed**: ligesom ethvert andet ondsindet program, kan ransomware udnytte sikkerhedshuller på din computers operativsystem eller i et program (f.eks. en webbrowser), der er installeret på din computer. (Derfor er det vigtigt altid at opdatere sin computer)

Populære Ransomware varianter (infektions metoder)

Som nævnt ovenfor, er der mange varianter af ransomware, men de kan groft inddeles i fire kategorier:

1. **SMS Ransomware**: Denne type af ransomware låser din computer og viser en besked med krav om løsesum og en kode. For at låse din computer op, bliver du bedt om at sende en kode via SMS til et overtakseret SMS nummer og du vil forhåbentlig modtage en tilsvarende kode for at låse den op.

Figur 1 – Eksempel på en SMS ransomware låse skærm.

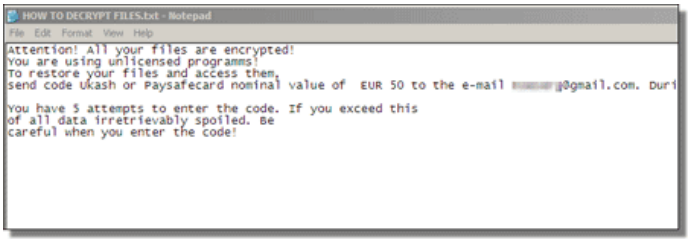
Figur 1 er et eksempel på en skærmlås, (som hævder at være fra Microsoft) der viser en af SMS ransomware varianterne. Låseskærmen instruerer ofrene til at sende koden (4121800286) til 3649 (som er en overtakseret SMS nummer) for at modtage Windows® aktivisering koden

2. **Winlocker**: Denne variant af ransomware låser også computeren, men den viser en mere truende løsesum besked, som synes at være fra en offentlig myndighed. I modsætning til SMS ransomware instruerer denne særlige form for malware dig i at betale via et online betalingssystem som Ukash, Paysafecard eller Moneypak

Figur 2 er et eksempel på en ny variant af Winlocker ransomware. Låseskærmen angiver, at FBI har låst brugerens computer idet han/hun angiveligt skulle have begået en form for cyberkriminalitet. Låseskærmen indeholder også instruktioner om, hvordan brugeren kan betale via en online betalingsservice. Denne type malware er mere almindeligt kendt som "FBI Virus" eller "Moneypak Virus

Figur 2 – Eksempel på Winlocker ransomware låse skærm.

3. **Fil kryptering**: Denne form for ransomware kan kryptere dine personlige filer og mapper ved hjælp af komplekse krypteringsalgoritmer der gør din computer ubrugelig. Malware forfatteren kræver derefter, at du betaler for en dekrypteringsnøgle, ved hjælp af en af de online betalingssystemer, der er nævnt ovenfor. Ransomware efterlader ofte en fil (eller en "løsesum notat") på offerets computer med betalingsinstrukser. Nogle af disse typer af ransomware låser din skærm, andre gør ikke.

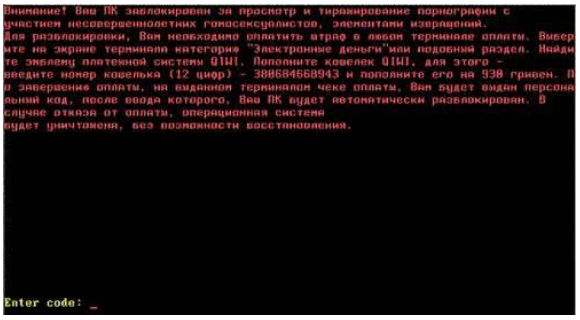


Figur 3 – Eksempel på en fil encryptor ransomware ransom besked/note.

4. **MBR Ransomware**: Dette er en anden populær variant af ransomware, men den går et skridt længere end de andre tre typer nævnt ovenfor med hensyn til hvordan computeren er låst. MBR Ransomware kan ændre computerens Master Boot Record (MBR) og afbryder normal boot-processen. MBR er en partition på computerens harddisk, der gør det muligt for operativsystemet at indlæse og starte. Når denne ransomware aktiveres, vises løsesum meddelelsen så snart

computeren er tændt, hvilket betyder at du ikke får mulighed for at indlæse operativsystemet for at fjerne infektionen og dermed reparere dit system

MBR Ransomware kan virke skræmmende, men denne type af infektion kan nemt fjernes. Meddelelsen siger ofte at filerne er blevet krypteret, men i virkeligheden, er de ikke.



Figur 4 – Eksempel på en MBR ransomware låse skærm.

Sådan fungerer det

Ransomware er en rentabel kriminel forretning, og dens succes ligger i måden den fungere på. Hele ransomware strategien går ud på at skræmme ofret ved at det ser ud som om det er offentlige myndigheder der har "låst" computeren og truslen om straf og eventuelt fængsel. For at deres angreb skal virke autentiske, har ransomware forfatterne (læs hackeren) brugt offentlige myndigheders logoer og geo-specifikke tjenester for at bestemme hvilket land den inficeret computer befinder sig i. C & C servere er centraliseret servere der bruges af cyberkriminelle til at fjernstyre inficerede maskiner ved at sende kommandoer og modtage output (data) fra maskinerne. Når visse typer af ransomware rammer computeren, afgør det, hvilket land du befinder dig i og sender data til C&C serveren. Serveren svarer med billeder, der bruges til at låse skærme. Disse billeder indeholder tekst skrevet i det lokale sprog og logoer fra offentlige myndigheder.

Hvordan du beskytter din Computer imod Ransomware

Den måde du beskytter din computer imod ransomware ligner de måder du beskytter din computer imod enhver anden form for malware. Her er et par regler du bør huske for at undgå malwareangreb:

1. **Foretag altid backup af dine data**: uanset om det er en ransomware eller andre malware-angreb, er der altid en mulighed for at du mister dine data. Regelmæssig Backup af dine data der opbevares et sikkert sted væk fra computeren, så kan du altid gendanne dine data i tilfælde af at du bliver inficeret af malware eller mister dem på en anden måde.
2. **Tænk før du klikker**: åbne ikke vedhæftede filer, du ikke havde forventet at modtage eller klikke på links på mistænkelige websteder. Hvis du kan se en e-mail fra en virksomhed, der forsøger at få dig til at åbne en vedhæftet fil for at modtage penge eller en gave, skal du ignorere denne e-mail, fordi det kan være et forsøg på at få dig til at installere skadelig software
3. **Sikre din PC**: Sørg for, at din computer er beskyttet med anti-virus/anti-malware-software.
4. **Vær opdateret**: Sørg for at alle dine sikkerhedsprogrammer, operativsystem og andre installeret programmer er opdaterede. Sørg også for, at automatisk opdatering er slået til.
5. **Betal ikke**: Hvis du mener at du er offer for et ransomware angreb, skal du ikke gå i panik, og hvad der er mere vigtigt, lad være med at betale. Selv hvis du betaler, er der ingen garanti for, at computerens funktionalitet eller dens data vil blive gendannet. I stedet skal du kontakte Rigspolitiets Nationale Cyber Crime Center (NC3). https://www.politi.dk/da/borgerservice/anmeldelser/hacking/

Og, husk at ransomware, eller enhver anden form for malware for den sags skyld, ikke er begrænset til computere eller Windows. Når det drejer sig om it sikkerhed, skal du sikre, at du holder alle dine enheder beskyttet (Smartphone, printer, router mv.). Hvis du har spørgsmål relateret til denne form for malware, er du altid velkommen til at kontakte os via vores kontaktformular eller blot efterlade en kommentar nedenfor. Vi hjælper dig naturligvis også gerne hvis du skulle være ramt af ransomware eller anden form for malware, men husk, der er større chancer for at løse din opgave hvis du har taget backup inden du er blevet inficeret.

Med venlig hilsen

NewTech IT Teknisk Support