Objava za medije

Datum: *17. svibnja 2017.*

Kontakti: *Jasna Kržanić, marketing i komunikacija*
Mob: +385 98 383 012

Tomasz Sawiak
Zamjenik direktora, Tim za računalnu sigurnost društva PwC
Tel. +48 519 504 234
tomasz.sawiak@pl.pwc.com

Manje od polovice društava spremno je za suočavanje s rastućom hakerskom prijetnjom

Stručnjaci PwC-a tvrde kako je opasnost od financijskih gubitaka zbog zlonamjernih softvera koji enktriptiraju podatke korisnika računala, poznatiji kao cryptolockeri ili ransomware, u porastu. Naglašavaju da samo polovica društava koje je PwC istražio ima alate za otkrivanje neovlaštenog ulaska i da aktivno nadgledaju i analiziraju podatke o informacijskoj sigurnosti, dok manje od polovice društava izrađuje procjene ranjivosti, procjene prijetnji i pretplaćeni su na usluge prikupljanja informacija o prijetnjama[1].

Hakeri neprestano unaprjeđuju svoje taktike, otkrivajući nove načine za izvlačenje novca od ciljanih poduzeća i pojedinaca. Prije samo nekoliko godina, glavna metoda bili su *phishing* napadi koji bi zarazili računala korisnika internetskog bankarstva, od kojih je traženo da preuzmu *malware* klikom na poveznice u elektroničkoj pošti. Nakon što bi ciljana računala bila zaražena, napadači bi pratili korisničke transakcije i krali njihove podatke u svrhu odobravanja neovlaštenih transakcija ili bi pomoću tehnika socijalnog inženjeringa na prijevaru nagovorili nesvjesne klijente da novac prebace na račune prevaranata.

„Napadači danas za izvlačenje novca sve više koriste nove metode utemeljene na iznudi", rekao je **Piotr Urban**, PwC-ov partner koji vodi interni tim za kibernetičku sigurnost. „Već nekoliko godina vidimo porast prijetnje ransomwarea. Nakon što je instaliran na računalo, taj softver enkriptira datoteke i zahtijeva od korisnika plaćanje naknade za dekripciju."

Ako korisnik ne plati naknadu, gubi pristup podacima ili ti podaci budu objavljeni, nanoseći štetu ugledu korisnika i njegove organizacije.

Velika poduzeća često izrađuju sigurnosne kopije podataka o korisnicima i proizvodnji, tako da se enkriptirani podaci mogu povratiti. Iako se na prvi pogled poduzeća na taj način čine otpornima na ovu vrstu prijetnje, to nije uvijek tako.

„Povrat podataka nakon što enkripcije putem ransomwarea samo je prvi korak", rekao je **Tomasz Sawiak**, zamjenik direktora tima za kibernetičku sigurnost. „Ugled društva također je važan i u opasnosti je ako se ukradene informacije objave ili ako se otkrije informacija o samom incidentu. Osim toga, napadači mogu instalirati druge komponente malware koje omogućuju daljinski pristup zaraženoj IT infrastrukturi, a da

[1] Izvješće PwC-a „The Global State of Information Security® Survey 2017": http://pwc.to/2qkinUZ, stranica 7.

ne spominjemo troškove prekida poslovanja zbog zaraze ili potrebu izoliranja sustava kako bi se problem riješio i umanjila prijetnja."

Kako WannaCryptor (WannaCry) ransomware funkcionira?

Epidemija zaraze WannaCry ransomwareom u porastu je od petka, 12. svibnja. Mnoga velika međunarodna društva pogođena su tim napadom.

Kao i u većini takvih slučajeva, računala mogu biti zaražena putem elektroničke pošte koja potiče korisnike da otvore privitke, ali ovaj napad razlikuje se mehanizmom samorazmnožavanja koji je ugrađen u malware i omogućava širenje zaraze s jednog računala na druga koja se nalaze u istom IT okruženju. Malware koristi poznatu sigurnosnu rupu u sustavu Windows koju je Microsoft zakrpio svojim ažuriranjem MS17-010 u ožujku. Nažalost, ažuriranja softvera i instalacije zakrpi zahtijevaju puno vremena u velikim IT okruženjima te mnoga računala ostaju ranjiva. Osim toga, računala s ranjivim sustavima Windows mogu se zaraziti povezivanjem na javne Wi-Fi mreže na koje su spojena druga zaražena računala. Malware se može automatski ažurirati te instalirati dodatne verzije koje izbjegavaju standardne metode otkrivanja antivirusnih sustava.

Osnovno je pravilo u ovakvim slučajevima (ako ne postoji prijetnja ljudskim životima) ne započinjati razgovor s napadačima i ne plaćati otkupninu.

Kako bi se ograničila opasnost od zaraze i rad malwarea WannaCry, važno je poduzeti sljedeće postupke:

- Brza izolacija zaraženih radnih stanica od ostalih dijelova IT infrastrukture poduzeća.
- Ograničavanje mogućnosti komunikacije komponenata infrastrukture s Internetom pomoću SMB protokola koji se koristi za prijenos i dijeljenje datoteka (blokiranje javne internetske komunikacije prema i od pristupnih točaka 137, 139 i 445).
- Ograničavanje mogućnosti korištenja SMBv1 verzije protokola za dijeljenje datoteka u cijeloj IT infrastrukturi.
- Ograničavanje mogućnosti pokretanja nepotpisanih makronaredbi u dokumentima programa Microsoft Office promjenom postavki pravila grupe i omogućavanjem samo odobrenih i pravilno potpisanih makronaredbi.
- Osiguravanje izvršenja daljinskog pristupa IT infrastrukturi putem VPN-a, koristeći potvrdu u 2 koraka (engl. *two-factor authentication*).
- Prepoznavanje i ograničavanje pristupa koristeći infrastrukturne komponente (bez instalirane zakrpe MS17-010) ključnim aplikacijama i komponentama IT infrastrukture poduzeća. Ugradnja zakrpe MS17-010 na sva ranjiva računala IT infrastrukture.
- Prisilna ažuriranja antivirusnih potpisa.
- Omogućavanje radnim stanicama da razriješe imena domena i komuniciraju s „kill switch" domenama korištenima u najpopularnijoj verziji malwarea WannaCry.
- Praćenje komunikacije i deblokiranje razrješenja za domene: iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com i ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com).
- Neprestana edukacija i podizanje svijesti zaposlenika o malwareu i vektorima napada koji uključuju elemente socijalnog inženjeringa.

O društvu PwC

Društvu PwC cilj je izgraditi povjerenje u društvo i rješavati važne probleme. Mi smo mreža društava u 157 država s više od 223.000 ljudi koji su predani pružanju kvalitetnih usluga iz područja osiguranja, savjetovanja i poreza. Saznajte više i recite nam što Vam je važno putem naše stranice www.pwc.com.

PwC posluje u Srednjoj i Istočnoj Europi posljednjih 25 godina. PwC u srednjoj i istočnoj Europi (PwC CEE) je mreža tvrtki koja se sastoji od zasebnih pravnih osoba u skladu s primjenjivim lokalnim zakonima i propisima. Nastojimo pomoći našim klijentima na lokalnim tržištima da postanu uspješniji i globalno konkurentniji. Danas imamo više od 8.800 ljudi, uključujući 260 partnera koji rade u 55 ureda u 29 država regije.

„PwC“ se odnosi na mrežu društava članova PricewaterhouseCoopers International Limited, od kojih je svako društvo zasebna pravna osoba. Za više informacija molimo posjetite stranicu www.pwc.com/structure.