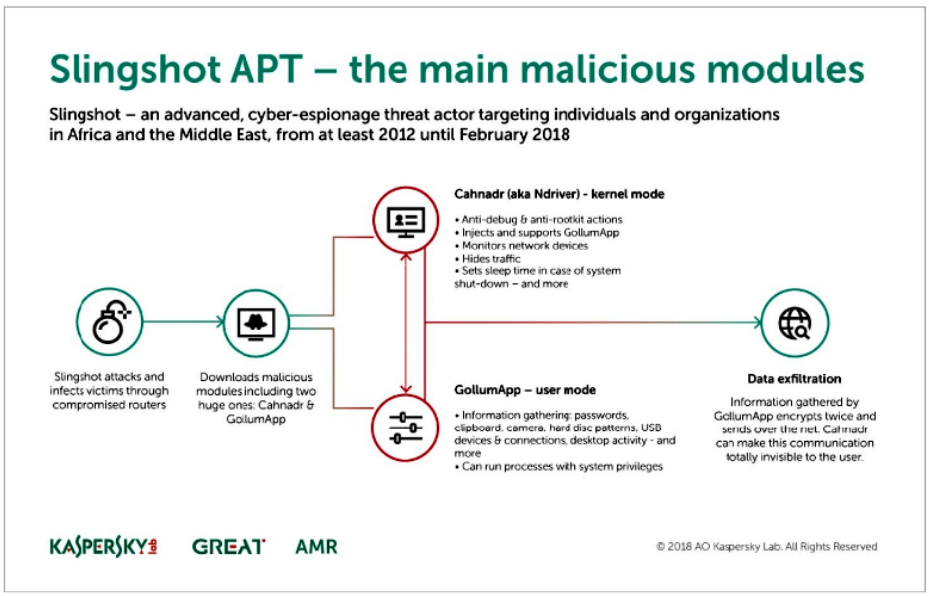
Ti si bila moja jedina

Slingshot je napredna računalno-špijunska prijetnja koja cilja na individualne i poslovne korisnike u Africi i Bliskom istoku, i to vrlo vjerojatno još od 2012. pa sve do veljače 2018. godine



Moduli od kojih se sastoji Slingshot i njihove funkcije

Rajko Plečko

Iz Kaspersky Security Analyst Summita (SAS) 9. ožujka stiglo je izvješće o još jednom slučaju visoko sofisticirane *cyber* špijunske kampanje pod imenom Slingshot ili po naški – Praćka! Prema nekim znakovima zaključili su da se radi o kompleksnoj i izvrsno dizajniranoj prijetnji koja je razvijana vrlo skupim alatima i prisutna je već dulje vrijeme. Imajući u vidu sve spomenuto, vrlo je vjerojatno da se radi o projektu koji je sponzoriran od neke vlade s ciljem o kojem možemo samo nagađati.

VEKTORI NAPADA

Kako bismo se mogli zaštititi od bilo kojeg napada, najprije je potrebno dijagnosticirati kako do njega dolazi. Slingshot se, kako bi inficirao ciljana računala, u nekim slučajevima oslonio na klasične slabosti Windowsa, no ono što je zapelo za oko, slučajevi su gdje je infekcija proširena kroz hakirane *routere* tvrtke Mikrotik.

Upravljanje i konfiguriranje Mikrotikovih *routera* moguće je odraditi preko web-sučelja, SSH konzole i uz pomoć male aplikacije temeljene na Windowsima Winbox, koja je većini korisnika najdraža zbog dobre preglednosti, lakoće korištenja i nezahtjevnosti. Sama aplikacija skida se sa stranica proizvođača ili sa samog *routera*, a kad ju prvi put pokrenemo i "napadnemo" *router*, s *routera* si sama skida određene DLL-ove koji se razlikuju ovisno o verziji Router Operating Systema (ROS-a) podignutog na konkretnom *routeru*. Napadači su pronašli način da na uređaje u taj sasvim legitiman paket ubace i maliciozne DLL-ove koje su korisnici prilikom konfiguriranja svojih uređaja ne znajući skinuli s *routera* zajedno s ispravnima. Ti su DLL-ovi kasnije poslužili kao *downloaderi* za različite maliciozne datoteke, koje su također spremili na *routere*.

Ovdje je važno reći da spomenute radnje nisu ni na koji način kompromitirale osnovne funkcionalnosti *routera*, koji je svoj posao i dalje obavljao besprijekorno. Također treba znati da je Mikrotik reagirao gotovo trenutačno, i problem, nakon što je prijavljen, riješio u vrlo kratkom vremenu.

Stručnjaci u Kaspersky Labu vjeruju da Mikrotik nije jedini brend koji je korišten u napadu Slingshot te da sigurno ima i drugih koje tek treba otkriti.

ELEMENTI NAPADA

Sve spomenuto samo je mehanizam za distribuciju stvarnog *malwarea* koji treba odraditi glavni posao, a u ovom slučaju radi se o dva mala programerska remekdjela: modulu koji radi u kernel modu i zove se Cahnadr, te modulu GollumApp, koji radi u korisničkom modu.

Cahnadr u kernel modu pruža napadaču potpunu kontrolu bez ograničenja nad cijelim inficiranim računalom, a za razliku od većine *malwarea* koji pokušava raditi u kernel modu, bez problema izvršava kôd, ne dovodeći se u situaciju da izazove BSOD. Na najnovijim verzijama Windowsa Cahnadr postiže kernel pristup uz pomoć vrlo inteligentne metode. Kako bi izbjegao Microsoftov Driver Signature Enforcement zahtjev, koji prevenira instalaciju nepotpisanih upravljačkih programa, Slingshot instalira starije verzije legitimnih programa, a nakon toga, uz korištenje njihovih poznatih ranjivosti, omogućuje Cahnadru pristup operacijama kernela. Drugi modul, GollumApp, još je sofisticiraniji i sastoji se od gotovo 1.500 funkcija.

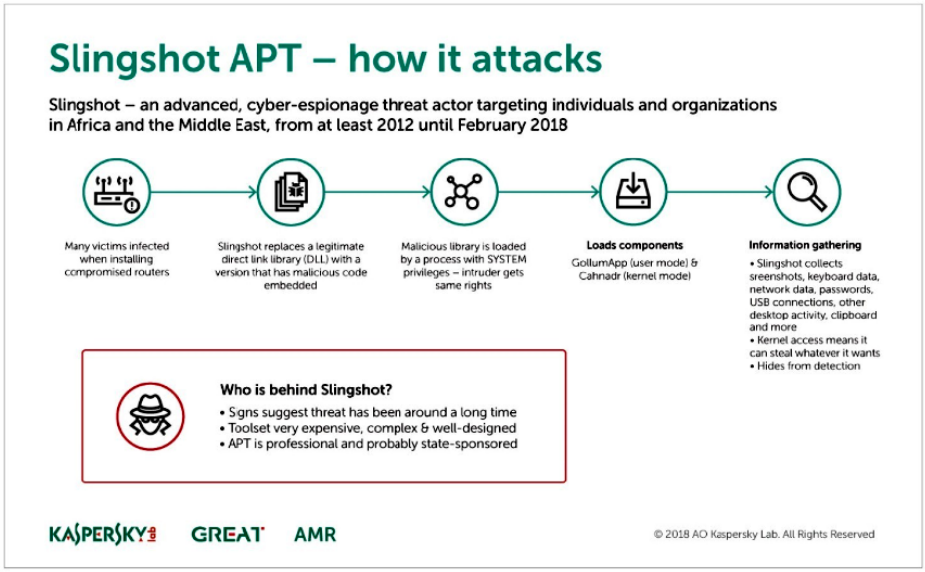
Zahvaljujući oboma, "Praćka" može sakupljati snimke zaslona, logirati unos s tipkovnice, prikupiti podatke o mrežnom prometu, uhvatiti upisane lozinke, razne aktivnosti na *desktopu*, *clipboardu* i mnoge druge nepodopštine, i sve to bez korištenja ijedne *zero-day* ranjivosti, što znači da nisu u pitanju nikakve nove i nepoznate slabosti OS-a.

Uzorci malicioznog kôda koje su stručnjaci ispitali, označeni su kao "verzija 6.x" što daje naslutiti da prijetnja postoji već

Praćka

dulje vrijeme. Za pretpostaviti je da su trajanje razvoja, potrebne vještine i cijena uključena u kreiranje takvog "sustava" vrlo visoki pa sve to navodi na zaključak kako se radi u pothvatu podržanom na razini neke od vlada, odnosno zemalja koje si takvo nešto mogu priuštiti te imaju potrebu za time. Kad se, pak, promotri geolokacija većine napadnutih sustava koji se uglavnom nalaze u zemljama sjeverne centralne i istočne Afrike te na Bliskom istoku, i neki elementi kôda koji pokazuju da je ugroza došla s engleskog govornog područja, izbor mogućih organizatora cijelog projekta još se više sužava.

Ono što Slingshot čini vrlo opasnim brojni su trikovi koje su njegovi autori iskoristili u cilju izbjegavanja detekcije. U trenutku kad nasluti da se nad računalom provodi neki oblik forenzike, u stanju je čak i zaustaviti izvođenje nekih svojih komponenata kako bi otežao detekciju. Nadalje, Slingshot koristi svoj vlastiti kriptirani datotečni sustav na neiskorištenom dijelu čvrstog diska.

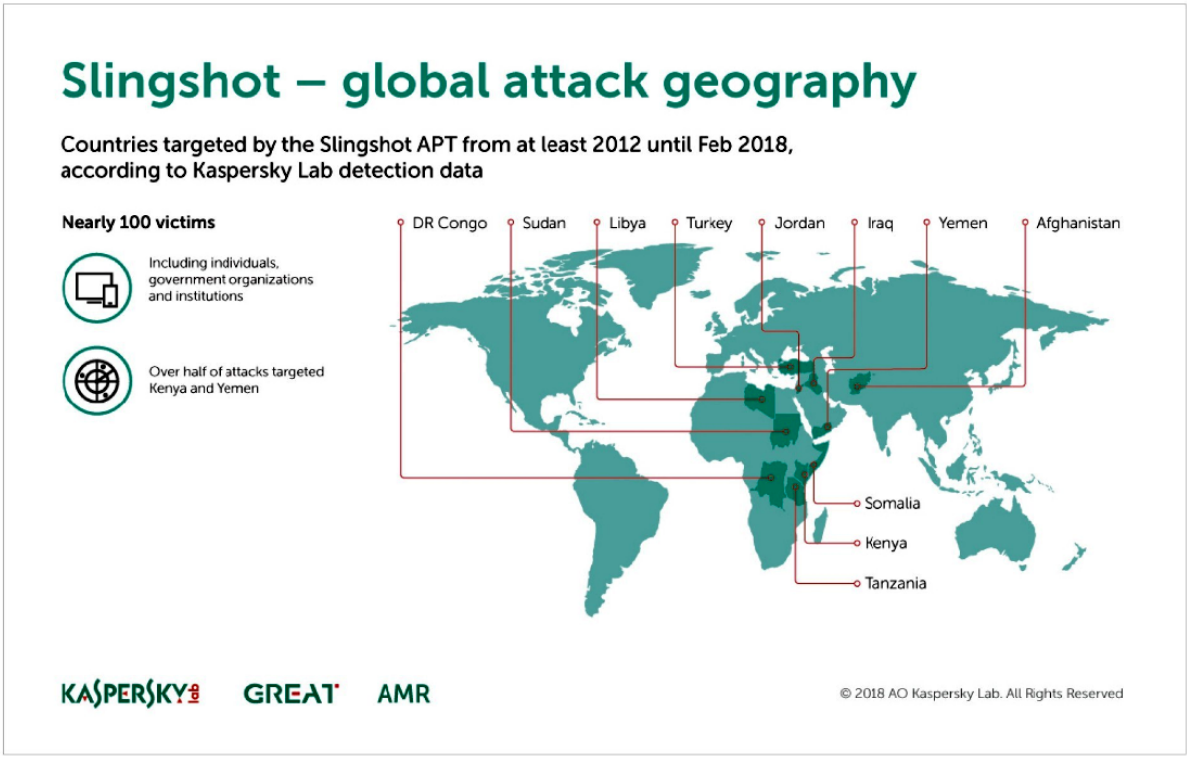


Redoslijed akcija na ciljanom sustavu koji vodi potpunom preuzimanju

KAKO SE OBRANITI

Ako koristite Mikrotikove *routere* i Winbox za upravljanje njima, skinite posljednju verziju programa sa stranica proizvođača i napravite *upgrade* ROS-a na najnoviji. Time ćete riješiti jedan od vektora napada, a "potpuno sigurnim" učinit će vas tek strateški pristup rješavanju problema. Kaspersky spominje svoju platformu Threat Management and Defense, a za vjerovati je da će i ostali proizvođači antivirusnih rješenja u najskorije vrijeme izbaciti i svoje varijante zaštite.

Kao što bi rekli profesori na faksu: za one koji žele znati više, preporučujemo pročitati cijeli forenzički nalaz, razvučen na punih 25 stranica (https://bit.ly/2pYPTPS).



Geografska lokacija većine napadnutih sustava daje naslutiti podrijetlo autora