Beste persrelatie,

SophosLabs Uncut heeft een nieuw rapport gelanceerd over Baldr, een malwarefamilie die in januari 2019 op ‘dark markets’ beschikbaar kwam.

Het volledige rapport **Baldr vs. The World** biedt een compleet inzicht en geeft meer informatie over de opkomst maar ook het verdwijnen van het deep web.

Tot nu toe was de informatie over Baldr meer dan schaars. Voor Sophos een uitdaging om de tanden erin te zetten; SophosLabs ging undercover om de activiteiten op het deep web te volgen. In het diepgaande rapport wordt de malware ontleed en onthult SophosLabs de innerlijke werking, opvallend cybercrimineel gedrag en ‘missers’ aan zowel de verkoop- als aankoopzijde. Enkele bevindingen:

* De Baldr-ontwikkelaars hebben het ontwikkeld voor entry-level cybercriminelen op het deep web en zij hebben als eerste PC-gamers getarget;
* Baldr is verder gegaan dan slechts gamers en heeft nu invloed op verschillende softwareoplossingen;
* Baldr gebruikt (net als vele soorten malware) codefragmenten die van andere malwarefamilies zijn ontleend. Baldr kun je zien als een ‘Frankensteinmonster’ dat is opgebouwd uit verschillende codefragmenten die van een relatief groot aantal andere malware is gebruikt;
* Baldr kan snel een breed scala aan informatie van zijn slachtoffers krijgen. Niet alleen wachtwoorden, data in de cache, configuratiebestanden en andere bestanden, cookies en uit een breed scala aan applicaties, waaronder:
* 22 verschillende webbrowsers
* 14 verschillende cryptocurrency-portefeuilles
* VPN-clienttoepassingen
* Hulpmiddelen voor bestandsoverdracht
* Instant messaging- en chatclients
* Gameclients en gaming-services, zoals Steam, Epic en Sony
* Services Gaming-aangrenzende services zoals Twitch of Discord
* Aanvallen reikten verder dan alleen gaming en infecties werden wereldwijd waargenomen. Volgens SophosLabs voeren deze landen het lijstje aan: Indonesië (21% van de slachtofferpopulatie), de VS (10,52%), Brazilië (14,14%), Rusland (13,68%), India (8,77%) en Duitsland (5,43%);
* Baldr's servercode omvatte bugs waarmee andere cyberaanvallers backdoors konden installeren om vervolgens wachtwoorden van klanten en data te stelen;
* Sommige klanten hebben hun servercode verkeerd geconfigureerd, waardoor hun tools en gegevens aan anderen zijn blootgesteld. SophosLabs ontdekte meer dan 150 logbestanden met gestolen data van computers van slachtoffers die per ongeluk naar de Total Virus-website waren geüpload;
* Onderzoekers denken dat de malware waarschijnlijk van Russische origine is en dat gegevens van slachtoffers in Rusland en de omliggende landen zijn opgeslagen in een speciale map op de commandoserver van de aanvallers;
* Baldr verdween in juni uit de handel na een woordenwisseling tussen bedenker en distributeur. SophosLabs verwacht dat het op den duur onder een andere naam weer de kop zal opsteken.

“Of Baldr een ‘vlam in een pan’ met een snelle piek, vervolgens zelf het slachtoffer werd van een ruzie tussen cyberdieven en zal terugkeren naar een langdurige dreiging, valt nog te bezien”, zegt Brian Schippers van Sophos in Nederland. “Het bestaan ​​ervan is echter een goede reminder dat zelfs gestolen stukjes malware aan elkaar kunnen worden geplakt om een ​​malwaremonster te creëren dat effectief kan zijn om in te breken, alles te graaien en het meteen op een lopen te zetten.”

Het rapport en een toelichting op de voornaamste bevindingen zijn terug te vinden op SophosLabs Uncut en Naked Security. Een directe link naar Bald vs The World is ook per heden beschikbaar. Mocht je naar aanleiding van deze mail interesse hebben in een telefonisch interview met de auteurs van het rapport, laat het mij weten. Ik zet het met veel plezier voor je op.

Groet,

Sandra van Hauwaert

Jacob-Jan Esmeijer