Lumen Newsroom

Black Lotus Labs révèle la distribution globale et la technique de dissimulation du botnet multi-outil Necurs

MONROE, Louisiane, 28 février 2019 /**PRNewswire**/ -- **CenturyLink**, Inc. (NYSE:CTL) renforce son engagement à protéger l'Internet des acteurs malveillants en partageant des renseignements sur le botnet Necurs découverts par sa nouvelle division de recherche sur les menaces et opérationnelle, **Black Lotus Labs**.

Découvrez le communiqué de presse multicanal interactif ici : **https://www.multivu.com/players/fr/8238355-centurylink-black-lotus-labs/**

Black Lotus Labs a pour mission d'exploiter la visibilité du réseau de CenturyLink pour protéger ses clients et assainir l'Internet. Pour ce faire, Black Lotus Labs repère et neutralise notamment les botnets tels que Necurs, un botnet de distribution de spam et de malwares particulièrement prolifique et étendu. Ce dernier a récemment adopté une technique de dissimulation lui permettant d'éviter d'être détecté tout en infectant discrètement d'autres bots.

Lire le rapport de Black Lotus Labs sur Necurs : https://www.netformation.com/our-pov/casting-light-on-the-necurs-shadow/

« Necurs est le multi-outil des botnets. D'un botnet émetteur de spam transmettant des chevaux de Troie et des rançongiciels bancaires il a évolué vers le développement d'un service de proxy et des capacités de cryptominage et d'attaques DDoS », a déclaré Mike Benjamin, directeur de Black Lotus Labs. « Ce qui est particulièrement intéressant est l'habitude régulière de Necurs de faire le mort pour éviter d'être détecté, avant de réapparaitre pour envoyer de nouvelles commandes aux botnets infectés, puis de refaire le mort. Cette technique est l'une des nombreuses raisons pour lesquelles Necurs a pu s'étendre à plus d'un million de bots autour du monde. »

Enseignements clés

- A partir de mai 2018, Black Lotus Labs a observé une cadence régulière de deux semaines d'arrêt suivies de trois semaines d'activité pour les trois groupes de bots les plus actifs qui constituent Necurs.
- Les quelques 570 000 bots de Necurs sont présents à l'échelle mondiale. Près de la moitié est située dans les pays suivants, par ordre de prévalence : Inde, Indonésie, Vietnam, Turquie et Iran.
- Necurs utilise un algorithme de génération de noms de domaine (DGA) pour rendre ses opérations opaques et éviter son démantèlement. Cependant, le DGA est à double tranchant : les noms de domaines DGA que Necurs va utiliser étant connus à l'avance, les chercheurs en matière de sécurité peuvent utiliser des méthodes comme le sinkholing des domaines DGA et l'analyse du trafic réseau et DNS pour lister les bots et l'infrastructure de commande et de contrôle (C2).
- CenturyLink a pris des mesures pour réduire le risque que présente Necurs pour les clients, et a également avisé d'autres propriétaires de réseaux des appareils potentiellement infectés pour contribuer à protéger l'Internet.

Ressources supplémentaires

- Découvrez comment TheMoon a évolué pour devenir un proxy en tant que service : **http://news.centurylink.com/2019-01-31-TheMoon-Illustrates-Evolving-Threat-of-IoT-Botnets**.
- Apprenez-en davantage sur l'attaque de deuxième phase de Mylobot : **http://news.centurylink.com/2018-11-14-Mylobot-botnet-delivers-one-two-punch-with-Khalesi-malware**.
- Découvrez comment le botnet Satori refait surface avec de nouvelles cibles : **http://news.centurylink.com/2018-10-29-Satori-botnet-resurfaces-with-new-targets**.

À propos de CenturyLink

CenturyLink (NYSE : CTL) est le deuxième plus important fournisseur de communications des États- Unis pour les multinationales. Ayant des clients dans plus de 60 pays et mettant un fort accent sur l'expérience client, CenturyLink s'efforce de devenir le meilleur fournisseur de réseau du monde en répondant à la demande croissante des clients pour des connexions fiables et sécurisées. L'entreprise est également un partenaire de confiance pour ses clients. Elle les aide à gérer la complexité croissante des réseaux et des technologies de l'information et leur fournit des solutions gérées de réseau et de cybersécurité qui leur permettent de protéger leurs entreprises.

Logo - **https://mma.prnewswire.com/media/134213/centurylink_logo.jpg**

For further information: LEWIS, Gaétane Roche, +33 1 85 65 86 27, CenturyLinkFrance@teamlewis.com

---

Additional assets available online: **(1)**

https://news.lumen.com/2019-02-28-CenturyLink-lance-Black-Lotus-Labs-sa-nouvelle-division-de-recherche-et-de-gestion-operationnelle-des-menaces