CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 08.04.2020 г.

Съдържание

Киберпрестъпници скриват злонамерен софтуер и сайтове за фишинг под SSL сертификати

07 април 2020

Повече от половината от първите 1 милион уебсайта използват HTTPS, но не всички криптирани трафици са безопасни.

Киберпрестъпниците все повече разчитат на SSL сертификати, за да създават на хората фалшиво чувство за сигурност при кликване на злонамерени връзки. Предположението, че HTTPS връзките и придружаващата икона за заключване предпазват служителите от атака, могат да застрашат бизнеса, ако не бъде осигурена надеждна SSL проверка.

Близо 52% от първите 1 милион уебсайта са достъпни през HTTPS през 2019 г. Почти всички (96,7%) онлайн посещения, инициирани от потребители, се обслужват през HTTPS; 57,7% от URL адресите в имейлите са HTTPS връзки. Това означава, че уеб прокси или защитната стена от следващо поколение - на която много фирми отдавна разчитат за видимост и контрол на достъпа онлайн, биха могли да пропуснат заплахите, присъстващи на злонамерени уебсайтове, ако SSL проверката не е активирана.

Няколко фактора предизвикаха възхода на приемането на HTTPS. През 2014 г. Google започна да включва присъствието на HTTPS в своите критерии за класиране на резултатите от търсенето. Уебсайтовете, обслужвани чрез HTTPS, имаха по-голяма вероятност да се появят в резултатите от търсенето в сравнение с останалите уебсайтове. Новите версии на Chrome и Firefox започнаха да предупреждават потребителите, че сайтовете не са защитени, ако не се обслужват през HTTPS. Бяха изпращани съобщения до потребителите на Интернет, че на уебсайтовете на HTTPS може да се вярва и целта беше да се мотивират предприятията да приемат HTTPS, за да могат да останат релевантни в класациите на търсачките.

За киберпрестъпниците е ежедневие да създават уебсайтове с отличието HTTPS. Органите за сертифициране като Let's Encrypt позволяват на уебсайтове, разработчици и нападатели да активират и автоматично подновяват HTTPS за своите сайтове, независимо от това дали те хостват законно съдържание или не. Стана ясно, че нови видове злонамерен софтуер се споделят зад символа на заключване, считан за защитен.

Изследвайки заплахите в уебсайтовете на HTTPS, изследователите откриха, че 47,1% работят с уязвим сървърен софтуер; например по-стари версии на Apache, Drupal или WordPress. Те откриха също, че 41,5% от уебсайтовете на HTTPS са категоризирани, а 10,7% са фишинг уебсайтове. Близо 67% от трафика без браузър -

който обикновено се генерира от агенти за крайни точки, които изтеглят актуализации, но също така включва и обратни повиквания на команда и контрол от заразени устройства - е под SSL.

Много е просто да хоствате фишинг връзки или да изтегляте драйвери за SSL, защото няма нищо, което да ги проверява. Това сочи за липса на SSL инспекция сред бизнеса и за произтичащи от това рискове. Повечето (92%) от имейл връзките, които потребителите щракват, се обслужват през HTTPS, включително както познати, така и неизвестни фишинг уебсайтове.

Организациите в някои вертикали се отказват от проверка на SSL поради причини за поверителност. Други фирми го избягват поради проблеми с изпълнението.

За повече информация:

https://www.darkreading.com/vulnerabilities---threats/cybercriminals-hide-malware-and-phishing-sites-under-ssl-certificates/d/d-id/1337504

Dark Nexus: забелязан е новопоявил се IoT ботнет злонамерен софтуер

08Април 2020

Изследователи по киберсигурността откриха нововъзникнала заплаха от типа IoT ботнет, която използва компрометирани умни устройства за извършване на атаки от типа „разпределен отказ от услуги“ (DDoS).

Ботът, наречен „dark_nexus“, работи, като атакува различни устройства, като рутери (от Dasan Zhone, Dlink и ASUS), видеорекордери и термокамери, за да ги включи в ботнета.

Досега dark_nexus съдържа най-малко 1372 бота, действащи като обратен прокси, обхващащи различни места в Китай, Южна Корея, Тайланд, Бразилия и Русия.

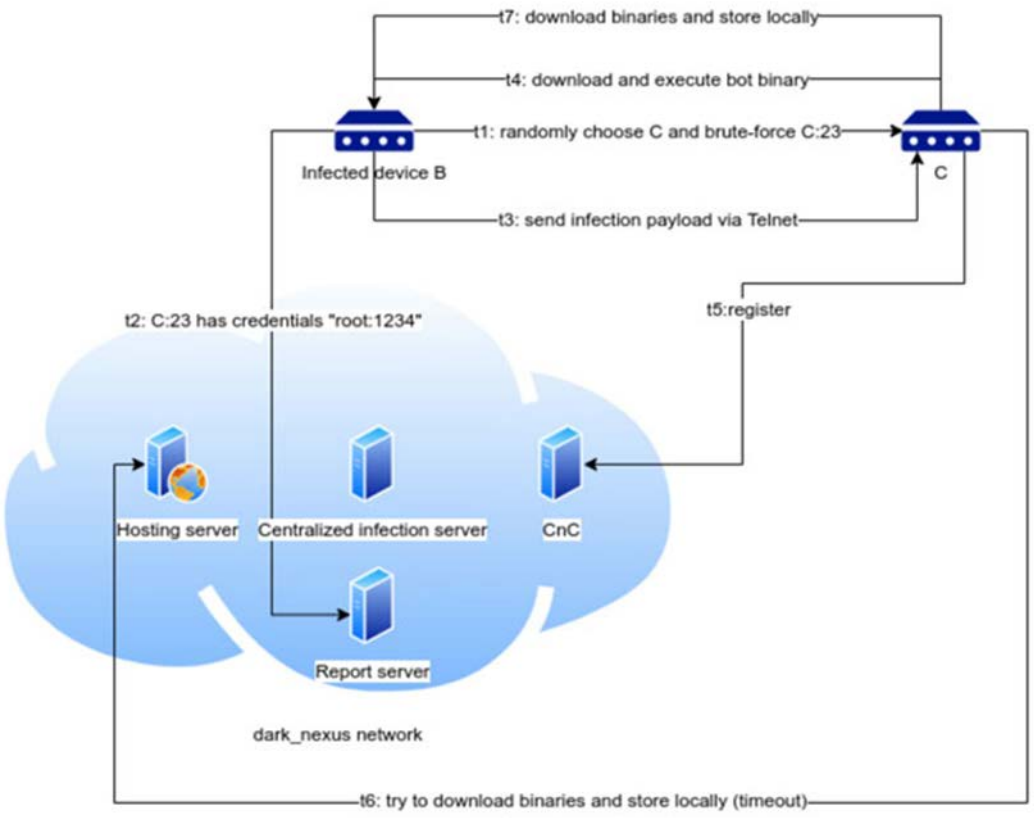
Въпреки че споделя някои функции с известни досега IoT ботнети, начинът, по който някои от неговите модули са разработени, го прави значително по-мощен и устойчив. Например неговите payloads се компилират за 12 различни CPU архитектури и се доставят динамично въз основа на конфигурацията на жертвата.

Вдъхновен от известни ботове като Qbot и Mirai

Стартовият код на бота наподобява този на Qbot: той се разклонява няколко пъти, блокира няколко сигнала и се отделя от терминала.

След това заприличва на Mirai - свързва се към фиксиран порт (7630), като гарантира, че само един екземпляр от този бот може да работи на устройството. Ботът се опитва да се прикрие, като променя името си на '/ bin / busybox.

Инфраструктурата се състои от няколко сървъра за командване и контрол (C2) (комутационни мрежи [.] Net: 30047 amd thiccnigga [.] Me: 30047), които издават отдалечени команди на заразените ботове и сървъри, на които ботовете споделят подробности за уязвими услуги (например устройства, защитени с пароли по подразбиране).



След като бруталната атака успее, ботът се регистрира на C2 сървъра, идентифицирайки CPU архитектурата на устройството, така че да предава персонализиран payload на зараза чрез Telnet, изтегляне на бот двоични файлове и други компоненти на зловреден софтуер от хостинг сървър (switchnets [.] Net: 80) и ги изпълнява.

В допълнение, някои версии на ботнет (4.0 до 5.3) идват с обратна прокси функция, която позволява на жертвата да действа като прокси за хостинг сървъра, като по този начин насочва заразеното устройство да изтегля и съхранява необходимите изпълними файлове локално, вместо да се налага да се свързва към централния хостинг сървър.

Това не е всичко. dark_nexus идва с постоянни команди, които не позволяват на устройството да се рестартира чрез спиране на услугата cron и премахване на привилегии към услуги, които могат да бъдат използвани за рестартиране на въпросното устройство. Той също така използва техника, предназначена да осигури "надмощие" над компрометираното устройство.

Уникално, dark_nexus използва система за оценяване, базирана на тегла и прагове, за да прецени кои процеси могат да представляват риск.

Ботнетът Mirai, откакто е открит през 2016 г., е свързан с редица мащабни DDoS атаки. Оттогава се появиха многобройни варианти на Mirai, отчасти поради наличието на неговия изходен код в Интернет.

Фактът, че dark_nexus е изграден върху основите на Mirai и Qbot, е доказателство за развиващите се тактики на операторите на ботнет и на неопитни хакери, което им позволява да добавят нова функционалност, като използват различни уязвимости в лошо защитени IoT устройства.

За повече информация:

https://thehackernews.com/2020/04/darknexus-iot-ddos-botnet.html