**Heimdall**

Анализиране на злонамереност от USB устройства за масово съхранение чрез вградена система

Автор:

Иван Златанов,

НТБГ

Научен ръководител:

Явор Папазов,

CyResLab

**Въведение:**

Универсалната серийна шина, позната още като USB, е един от най-разпространените стандарти за серийна комуникация, който е приложен в голяма част от модерните компютъроподобни устройства. Концепцията му е предоставяне на асинхронен интерфейс за множество устройства, свързани към общ гостоприемник (host).

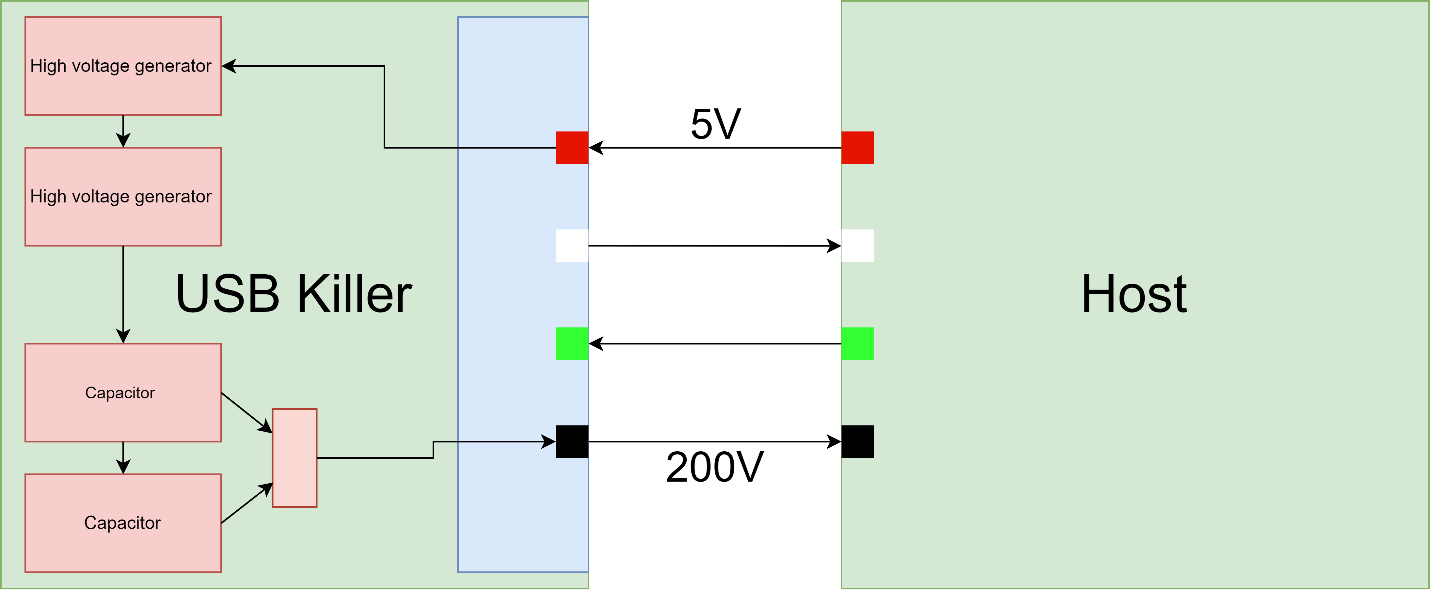
Голяма част от устройствата за масово съхранение (УМС) на пазара използват USB интерфейс, за да се свързват с хостове, които поддържат USB клас стандарта за УМС. Голяма част от тези устройства са малки, с голям капацитет и с висока скорост за изпълнение на I/O операции. Тези техни характеристики ги прави перфектния инструмент за разпространение и изпълнение на кибератаки.

Въпреки популярността на универсалната серийна шина, използването на устройства за масово съхранение, които имплементират интерфейсите ѝ, е ограничено или напълно забранено в съоръженията на множество правителствени и частни организации поради рискa за сигурността, който те представляват. УМС могат и са били използвани в множество кибератаки по целия свят. Съществуването на флашкоподобни устройства като USB killer-и, BadUSB-та и Rubber Ducky-та демонстрират как нетрениран персонал може перманентно да разруши сегменти на компютърни системи. Заради гореспоменатите причини Пентагонът, NASA, IBM и множество други са забранили използването на USB устройства за масово съхранение в техните съоръжения.

Stuxnet, Flame и BadUSB доказаха истинските възможности на такъв тип атака и, че USB УМС атаки могат да бъдат съчетани със системни слабости и да доведат до големи финансови и материални загуби. Въпреки всичко това, проблемът със сигурността на USB остава слабо адресиран.

Heimdall е решение на този проблем. Съчетавайки множество софтуерни и някой хардуерни тестове, проектът успява да изгради точна и сигурна система за анализиране на злонамереност от USB устройства за масово съхранение към техния хост.

**USB вектори за атака:**

*Насилствен токов удaр* – съществуването на устройства, наречени USB Killer позволява изпълнението на токов удaр към гостоприемника на устройството. Тези атаки са използвани за повреждане на компютри, смартфони, игрови конзоли и дори коли. USB killer-ът работи, като събира и зарежда във високоволтови кондензатори токът на порта, след което изпуска ~200 волта по релсите му за данни. Изображението е базова диаграма на USB Killer.

*Злонамерено променен фърмуер* – промяната на фърмуера на USB устройства за масово съхранени се изпълнява чрез изтекли инструменти като Patriot. Това действие може да накара обикновена флашка да заразява файлове по време на трансфера от нея към компютър или да ѝ предаде чужди функции и да я превърне в BadUSB.

*Сигурни* *Linux дистрибуции със задни вратички* – сигурни Linux дистрибуции като Tails могат да бъдат компрометирани чрез злонамерени kernel модули, поставени в initial ramdisk (initrd) файлът. Целта на initrd е да позволи изпълнението на startup процеса в две фази, където ядрото идва с възможно най-малко вградени модули. Нужните модули се прекачват от initial ramdisk-а към kernel-а. Ако някой от тях е злонамерен, то атакуващият ще има пълен достъп до компютъра на жертвата си.

**Функционалност:**

Проектът се състои от Python приложение, което живее върху модифицирано Raspberry Pi 3 Model B+.

Приложението чака включване на устройство за масово съхранение и задейства функциите му спрямо порта, в който e включеню. Някои от портовете са резервирани за тестови устройства, а други за сервизни (мишки, клавиатури и др.). Тестовите биват предадени на анализатора, който извършва тестовете върху тях. За манипулация и контакт с устройствата, файловите им системи и фърмуерите им се използват библиотеките Libusb1 и PyUdev.

Тестовете валидират информация на производителя, цялост на фърмуера, тестват вида на устройството, засичат задни вратички в Tails, вируси и USB Killer атаки. Част от тестовете се изпълняват и на други операционни системи чрез KVM Passthrough.

**Използвани технологии:**

Python - интерпретируем, интерактивен, обектно-ориентиран език за програмиране, създаден от Гуидо ван Росум.

C - език за програмиране, разработен от Денис Ричи в периода 1969 – 1973 г. Разработката на езика е тясно свързана с операционната система UNIX, чието ядро впоследствие бива пренаписано на езика C.

Libusb1 – Python binding популярната библиотека libusb, която предоставя директен достъп до USB устройства, свързани към компютър.

PyUdev – Python библиотека за наблюдение и контрол на udev events при Linux-базирани операционни системи.

PyQt – Python библиотека за създаване на графични потребителски интерфейси.

Raspberry Pi 3 Model B+ - серия от едноплаткови компютри с размери на кредитна карта, разработена в Обединеното кралство от специално създадена за целта фондация (Raspberry Pi Foundation) с цел популяризиране на обучението по основи на компютърните науки в училищата.

**Заключение:**

Heimdall e решение за опасен и съществуващ, но слабо адресиран проблем в киберсигурността, който имат частни и правителствени организации. Проектът съчетава хардуерни и софтуерни проверки, които са създадени специално за анализ на USB устройства за масово съхранение. Така се създава една сигурна и функционираща система.