A1

Easy To Use PDDOS

:Burner Phone DDOS 2 Dollars a day:70 Calls a Min

Weston Hecker Security Expert

Systems Network Analyst/Penetrations Tester/President Of Computer Security Association Of North Dakota

Slide 1

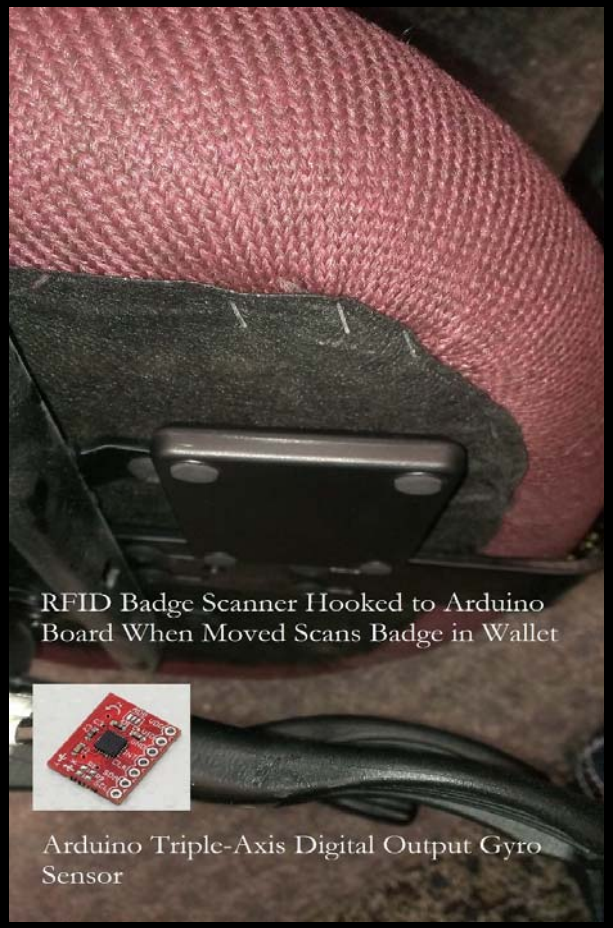
A1 Author, 9/16/2013

Who am I and what is this talk about?

- About Me: Penetration Tester, Computer Science/Geophysics, Tons of Certs, Custom exploits written for PMS Hotel Software, Two-way reservation fuzzing, and RFID Scanner that mounts under chair.
- About 9 years of pen-testing, disaster recovery, security research
- NERC, FFIEC, ISO, GLBA and FDIC, Compliance audits HIPPA, Omnibus
- Wrote custom exploits and scripts for obscure Internet Service Provider gear
- Tools of the trade “Fleet of Fake iPhones”
- The creation of a Phone Call Bomber from your Grama’s prepaid phone to a solar powered hacker tool hidden in light fixture at a public library
- Screen shot demonstration of 15 phones taking down a 200 person call center
- Distributed Denial of service Phone Systems “What it is how its used” “How it Effects Businesses”
- Alternate uses once phone has been flashed into attack platform.

Fleet of Fake iPhones With Teensy 3.0

RFID Badge Reader.



What is DDOS and TDoS? How do they differ?

- (**DDoS**) **attack** is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

- Telephony Denial of Service or **TDoS** is a flood of unwanted, malicious inbound calls. The calls are usually into a contact center or other part of an enterprise, which depends heavily on voice service.

  - Definition pulled from Wikipedia.com

Instances of TDOS

- Bank fraud “CNP” Theft
- Bank transfer mule scams
- Unintentional from spoofed scammer CID
- Call center attacks
- Politically motivated activism

Current Methods of TDOS

Caller ID Spoof Reflection Attack

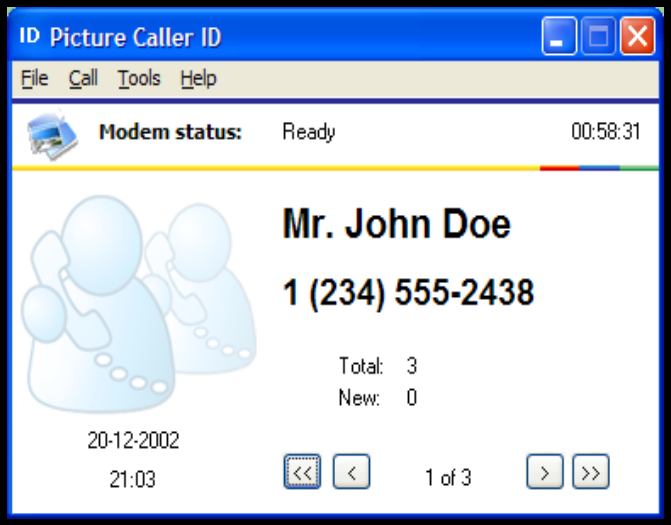
Malware on phones and call management software

Hijacked PRI and SIP Services WarDialing

Script to load caller information onto realtor webpage

Caller ID reflection attack

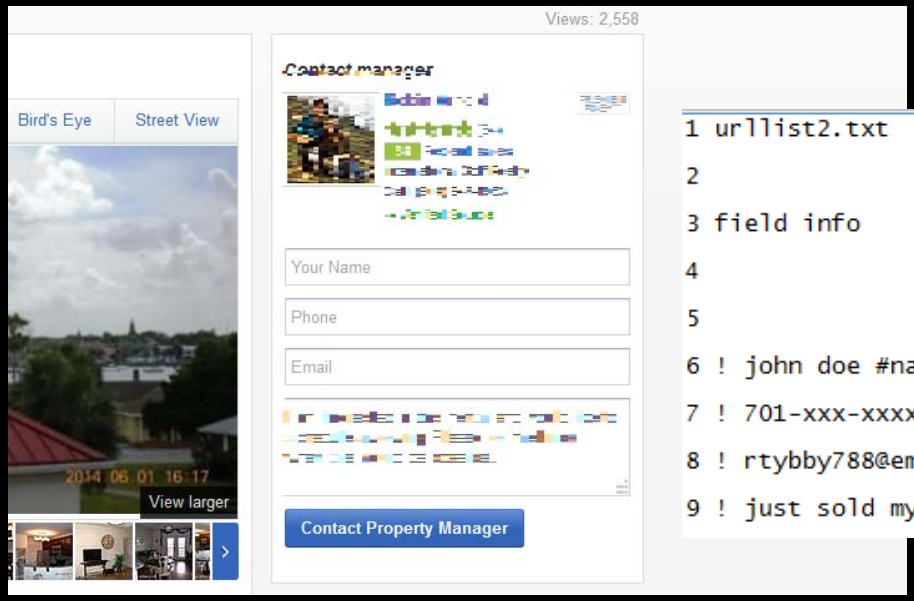
Legitimate phone service with spoofed Caller ID information



Thousands of calls returned to the number that they believe called them

Using salesmen to TDOS for you.

Page with generic templates.
Input fields automatically filled in.



Input for script, list of URLS and information off of input field.

```
1 urllist2.txt
2
3 field info
4
5
6 ! john doe #name
7 ! 701-xxx-xxxx #phone
8 ! rtybby788@emaildomintest567.com  #email
9 ! just sold my house in nevada looking at homes in the area please call#comment box
```

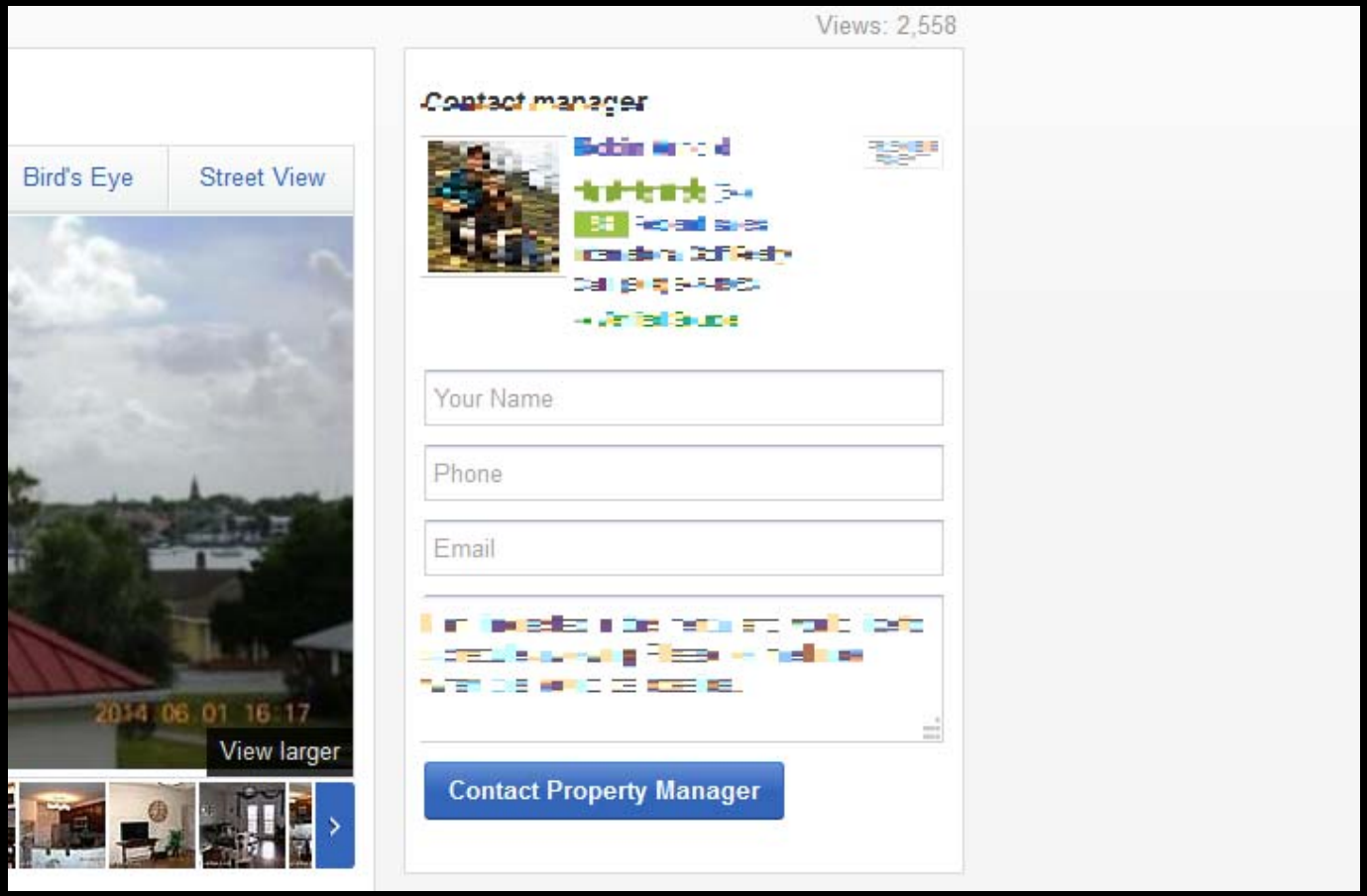
List of 4500+ pages that are auto populated from a text dump from realtor key work crawl.

```
1 urllist2.txt
2
3 field info
4
5
6 ! john doe #name
7 ! 701-xxx-xxxx #phone
8 ! rtybby788@emaildomintest567.com  #email
9 ! just sold my house in nevada looking at homes in the area please call#comment box
```

Web Crawling Bots

76% of Realtor Webpages use the same scripts don't use captchas

Script posts to 4600+ realtor pages in 2hrs.



Botnets of infected smart phones

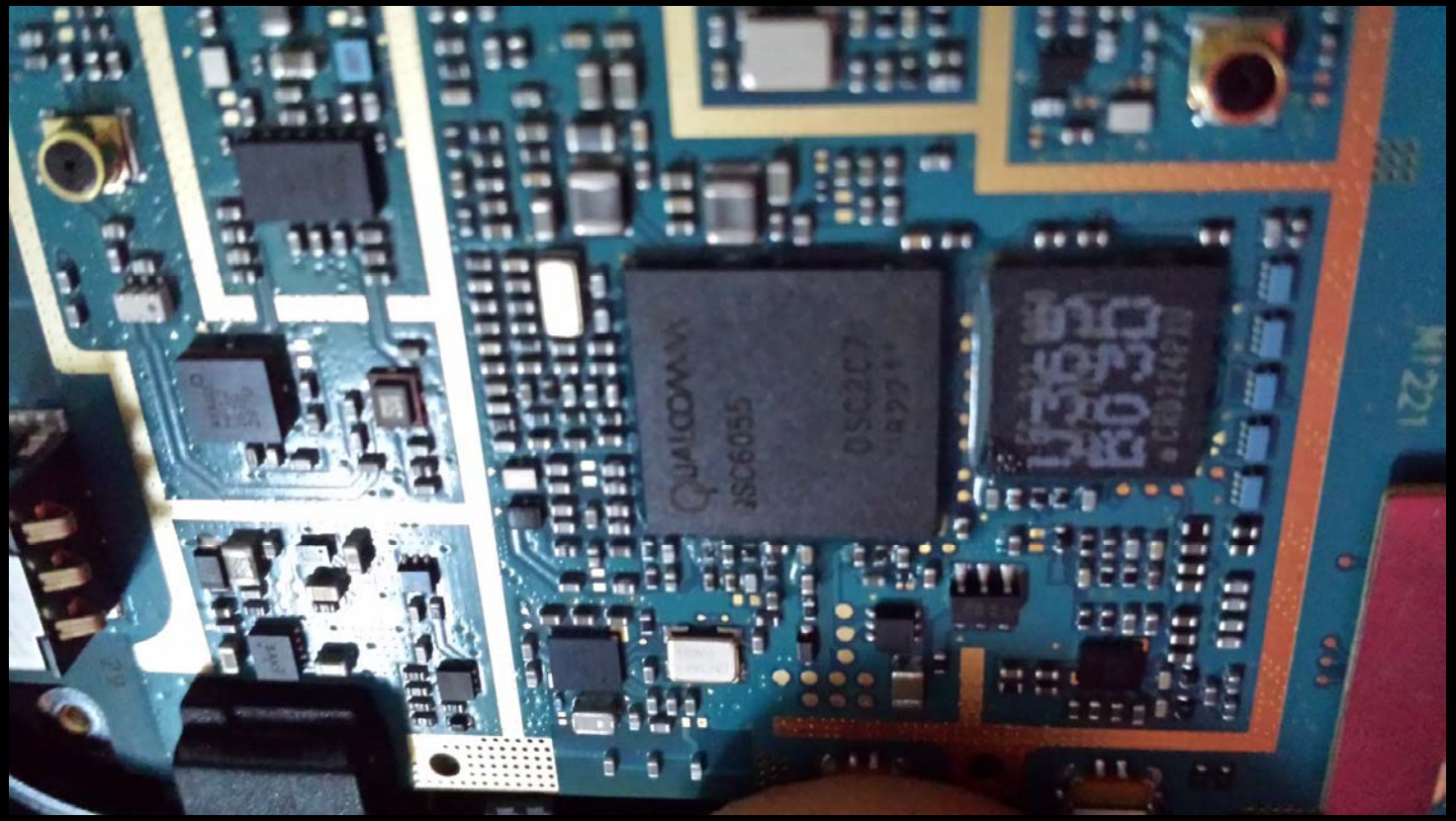
Just like computers smart phones have become a platform for botnets.

Increase in “rooted” phones opens doors to security risks.

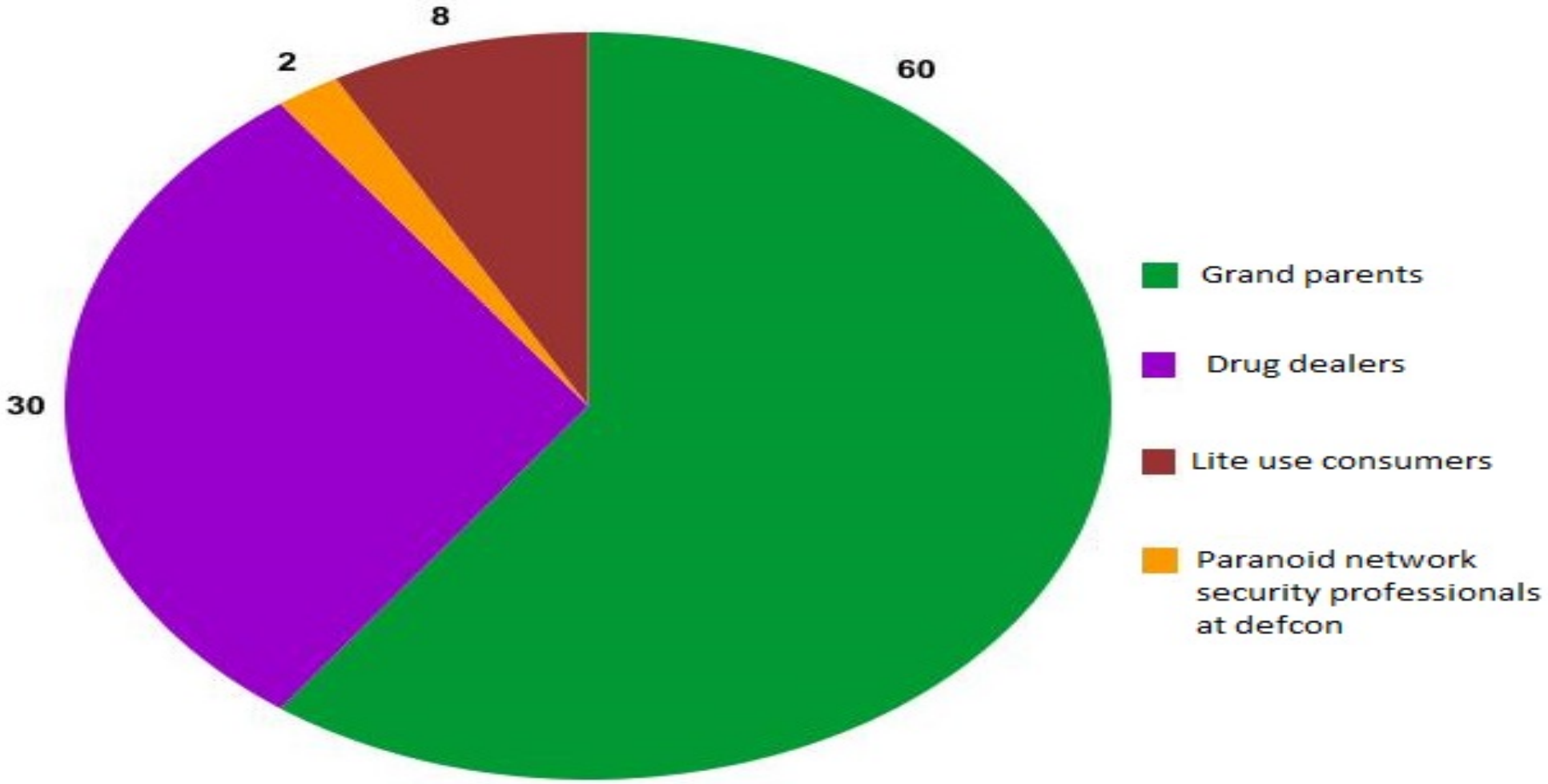
How I developed a Weaponized OEM cellphone platform

Prepaid Cell Phones Running Brew 3.1 Operating Systems CDMA 1X 800/1900 MHz Digital Only Samsung U365 aka Gusto-2

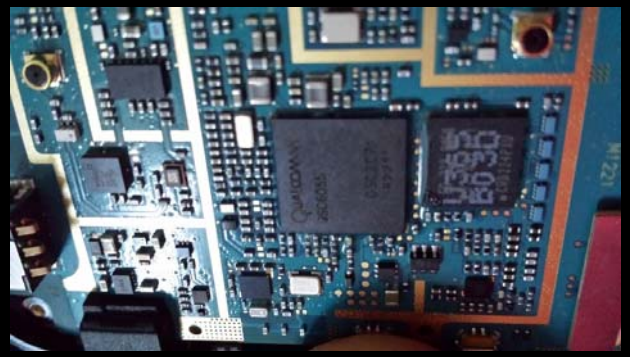
QSC6055 192MHz processor, Weaponized platform
Works on all value tier Qualcomm QSC60XX.



Pre Payed Phone Use Personal Study 2014

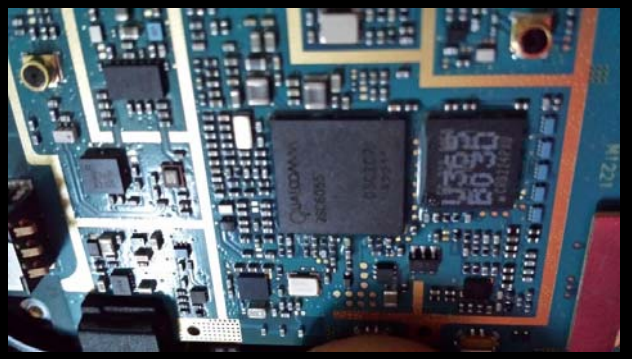


QSC6055 192MHz processor. Comes with Secure Boot, SEE, SFS



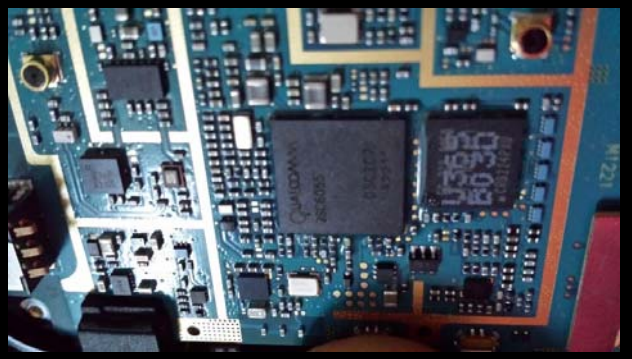
The developer editions of these models support boot loader unlocking, allowing the user to voluntarily void the manufacturer warranty to allow installation of custom kernels and system images not signed by authorized parties. However, the consumer editions ship with a locked boot loader, preventing these types of modifications. Until now…

No application processor very easy security to bypass. (Explained)
Great Easy Development Software.



Written in C/C++
BREW provides the ability to control voice mail and the activation or deactivation of devices by BREW applications. This capability will be provided by default if the UI is runs on top of BREW. The developer will provide the capability to program values for the set of BREW configuration parameters using the Product Support Tool (PST).

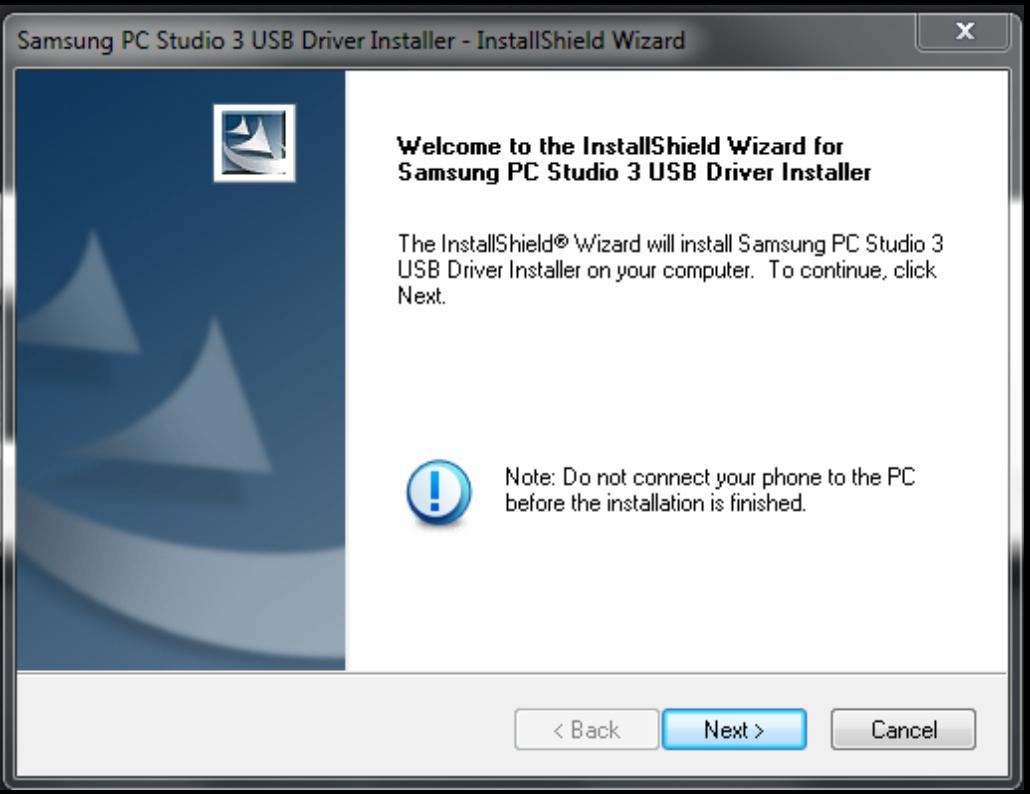
Exploit In IRingerMgr allows for interaction with clam and speaker manipulation such as picking up call instead of playing a ringtone.

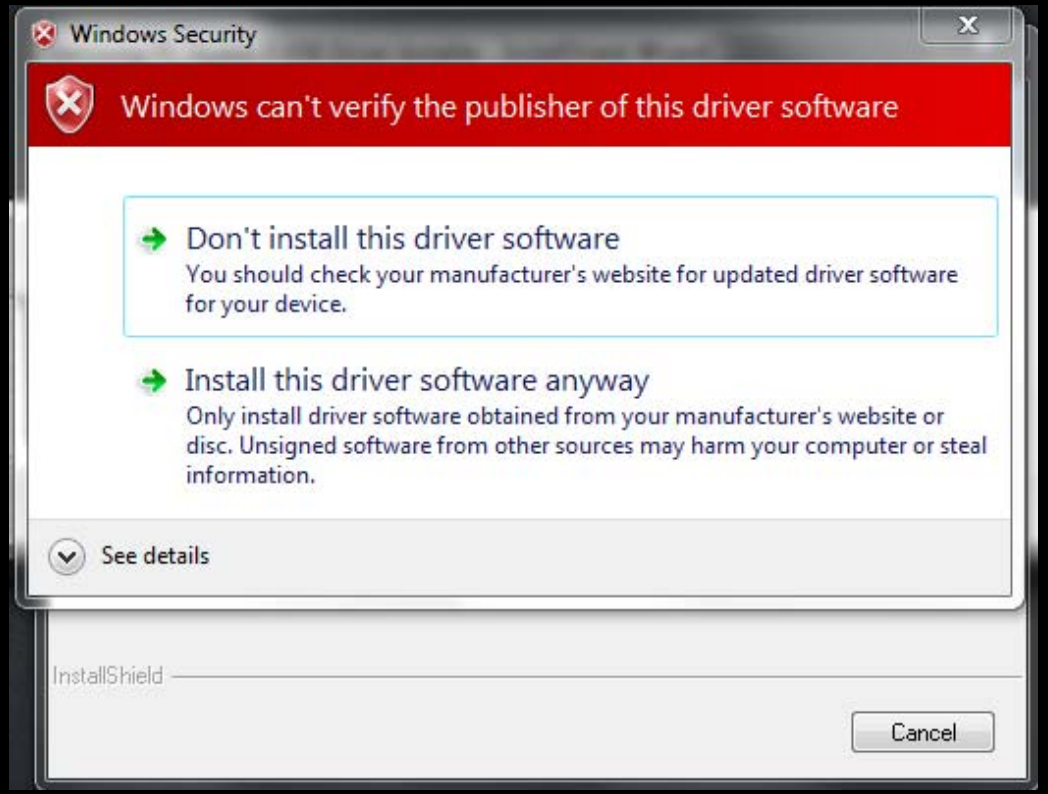


BREW provides the IRingerMgr interface that allows a developer to integrate their native ringer application with BREW. This enables BREW application developers to download ringers and manage ringers on the device. IRingerMgr allows assigning of ringers from a BREW application to be active and utilized for incoming calls (particular categories).

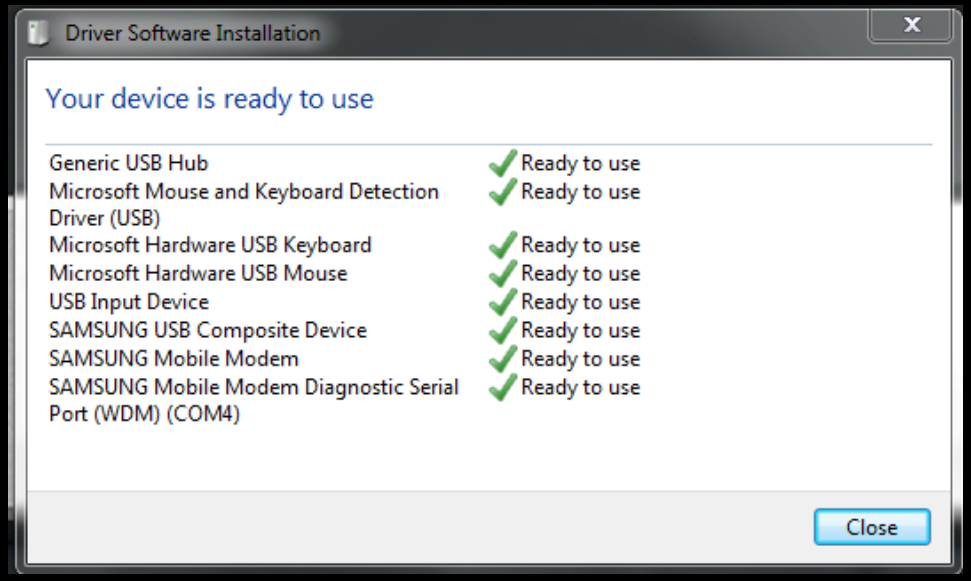
Clam-type phones refer Flip phones. On these devices, some Applications, multimedia applications for example, may need to alter their functional use of hardware or services.
So the ringtone payloads are able to bypass triggers and events caused by phone hardware provided by the device depending upon events generated by the action of the user.
Secondary display For devices supporting a secondary display, the display will be made available to applications requiring display services when the clam is closed. So the phone is still able to be fully interacted with at no additional battery cost.

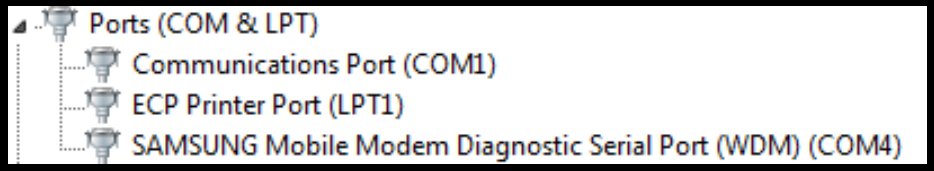
Modified executable allows for the software to be pushed to the device bypassing security feature easily using a loop hole within the certificate expiration process.

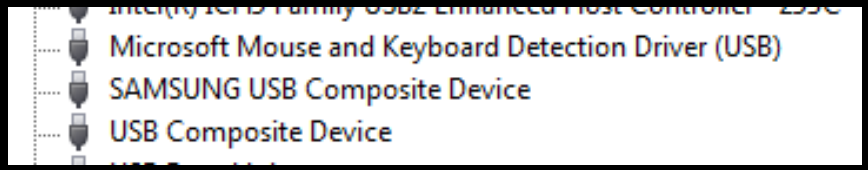




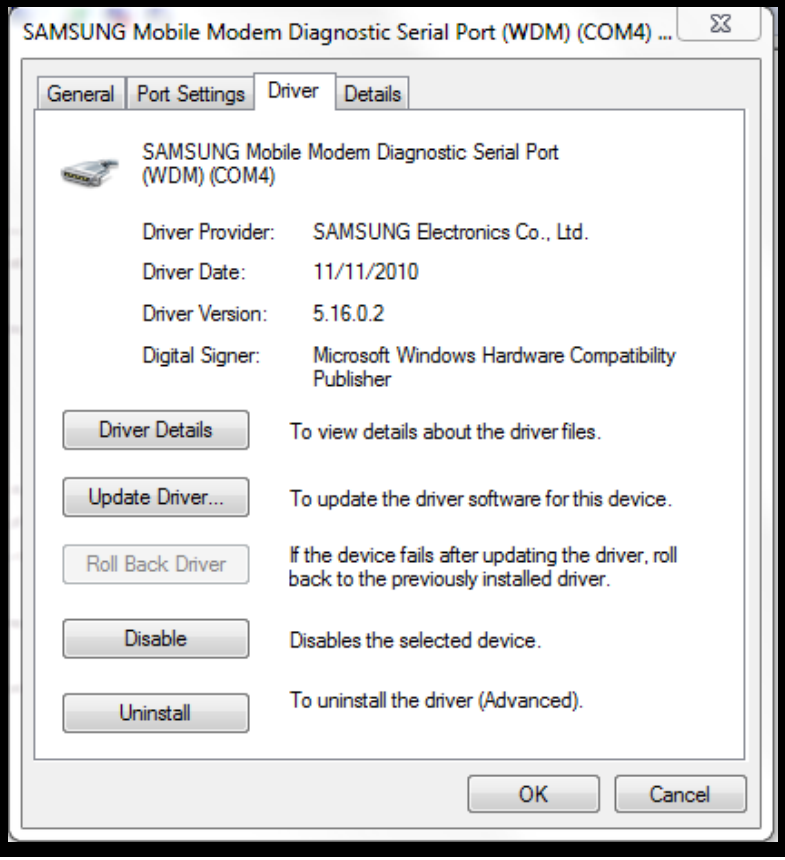
This error is exploited by running the modified executable while the other device is installed with a valid signed driver.

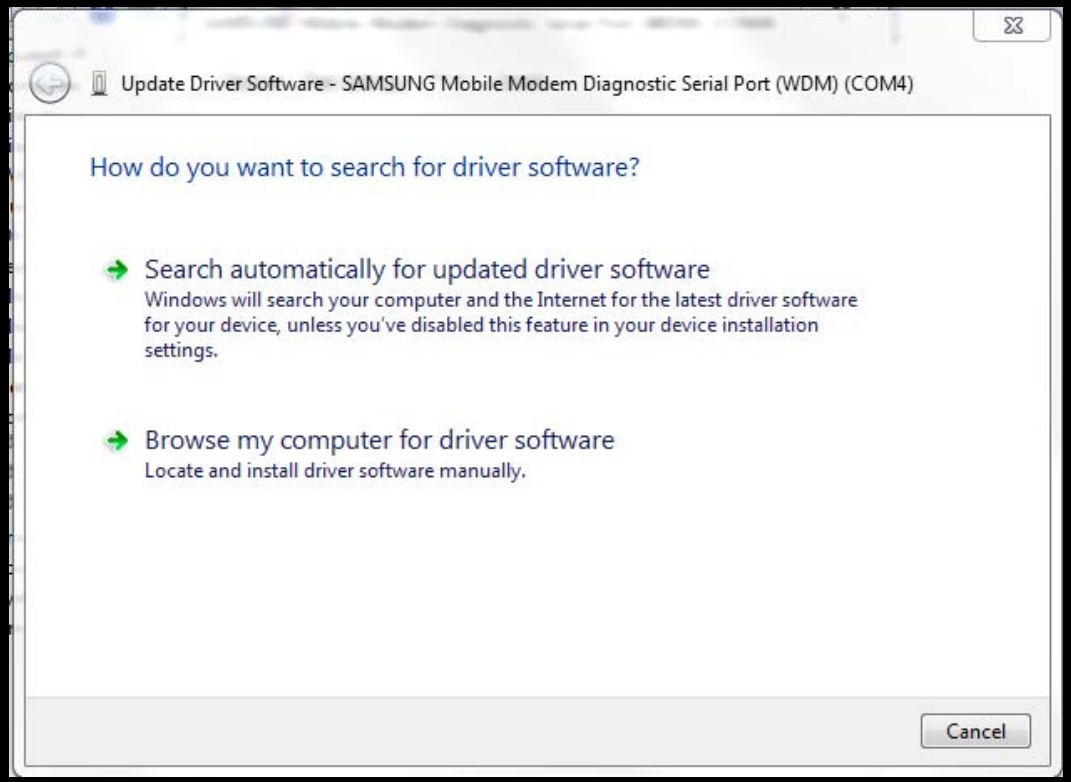




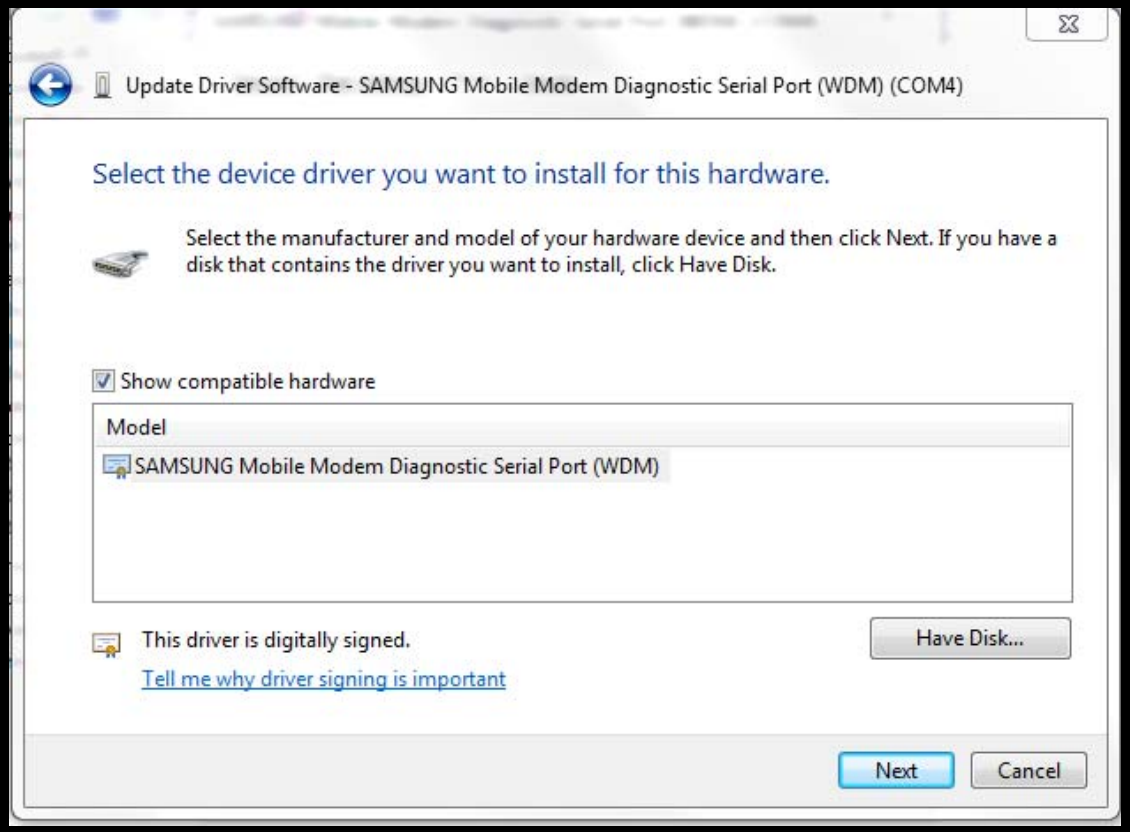


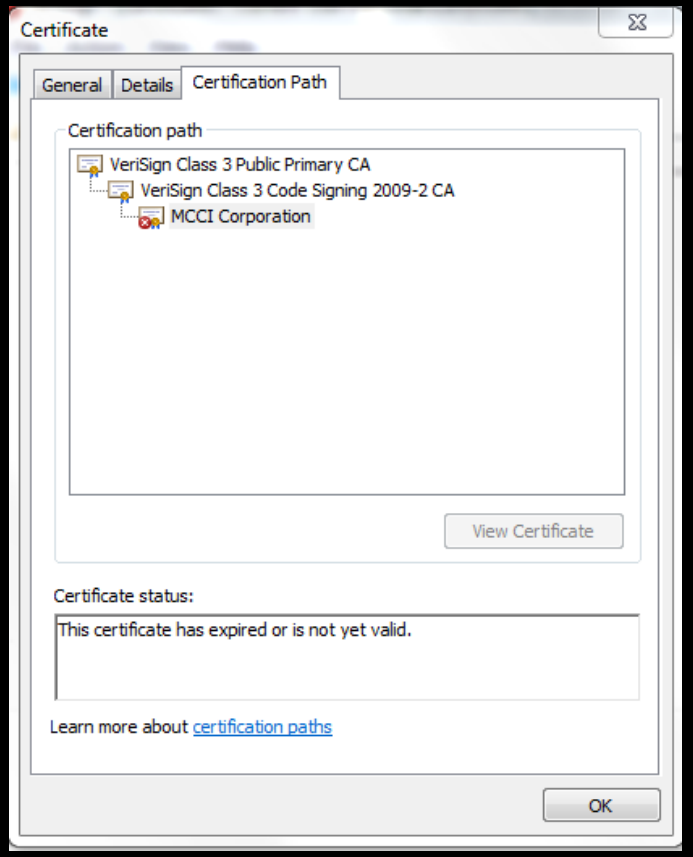
Once the driver is updated on the PC this allows full attack surface support.



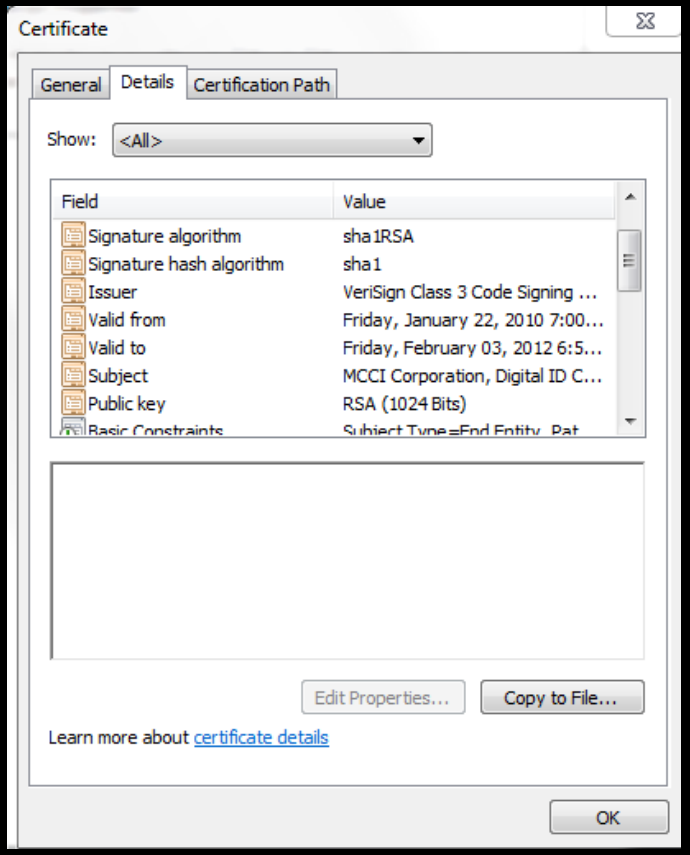


Drivers and device information are supported by a now expired certificate.





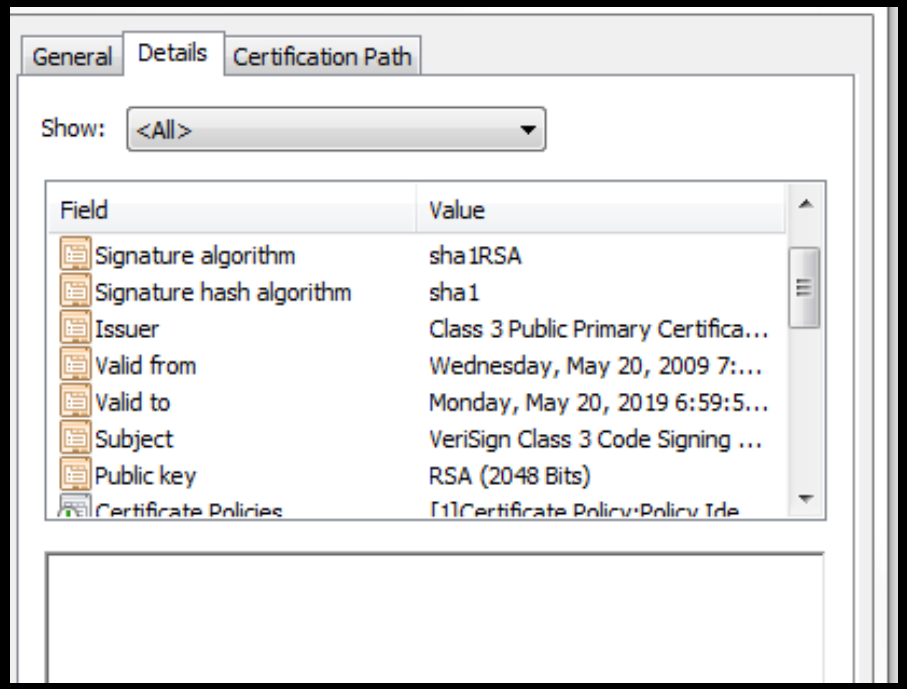
Certificate expired in 2012 which allowed me to bypass security feature sets.

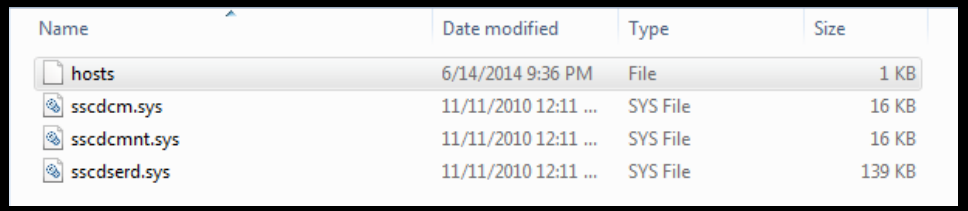


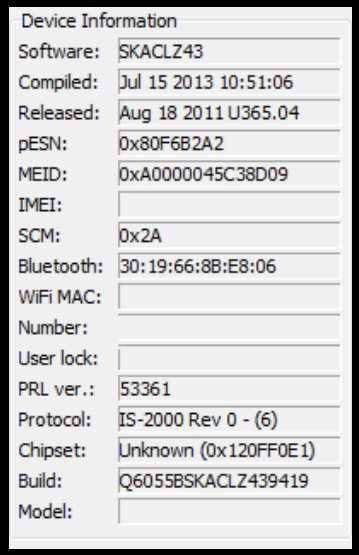

```
MCCI(r) USB Communications Enumeration -- V5.16 build 2702 (Nov 10 2010 15:09:56)
```

```
ERROR

+CME ERROR:
+CMS ERROR:
CONNECT
      CONNECT

BUSY

NO ANSWER

NO DIALTONE

NO CARRIER

>
```

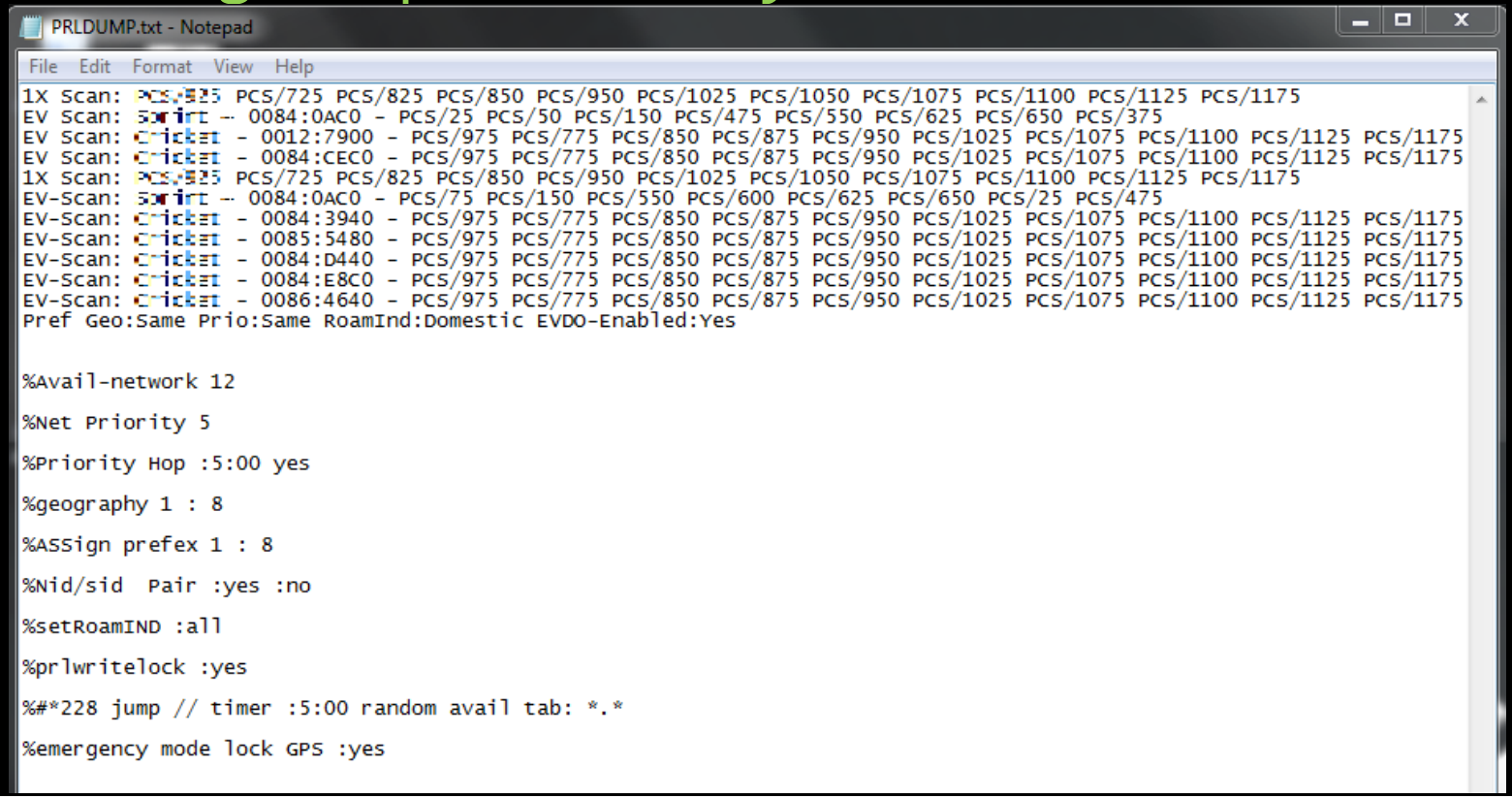
Modified driver files allow modifications of all device information.





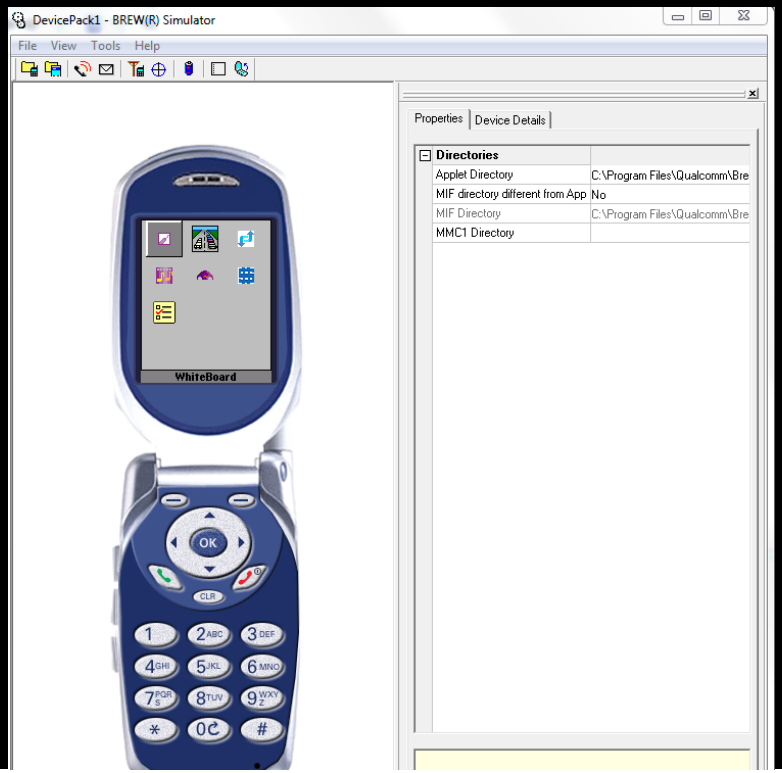


PRL (Preferred Roaming List) are pulled from the device activity. You can set jump time of the PRL list and turn off or lock the GPS position of the device making it practically untraceable.

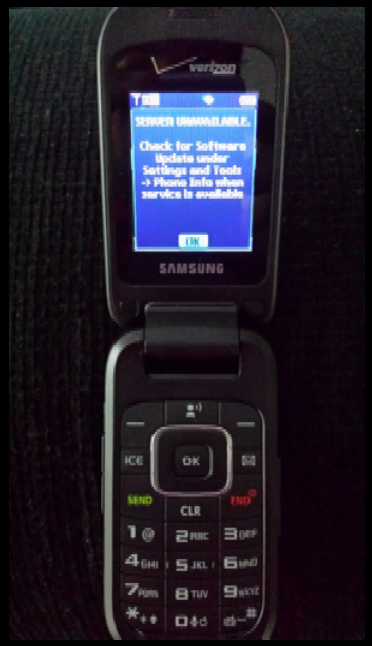


You can develop applications for the attack platform by emulating the software on custom written platform emulators provided for OEM developers

Full platform for emulation of U365 device

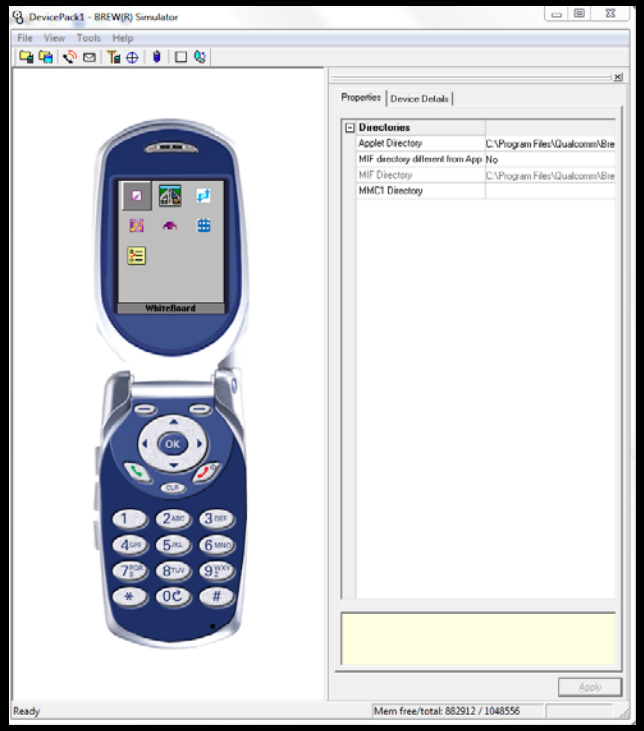


Testing your applications without having to load them on the device. This effectively makes it a development handset attack platform

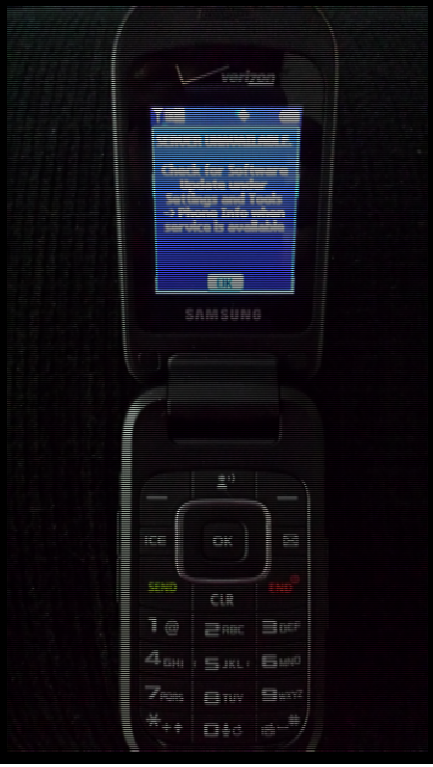


Now that you have your own fully unlocked platform, what now…

OEM Development Platform



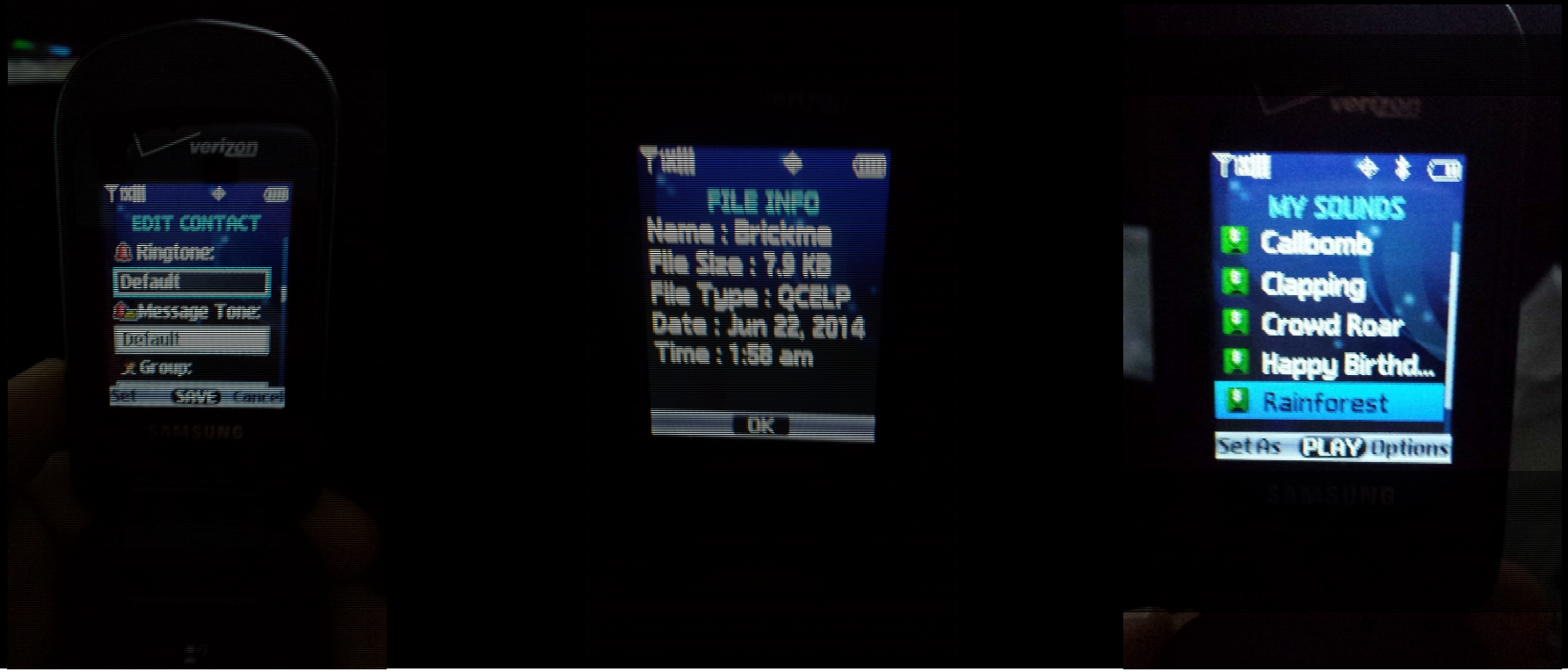
Weaponized Development Platform



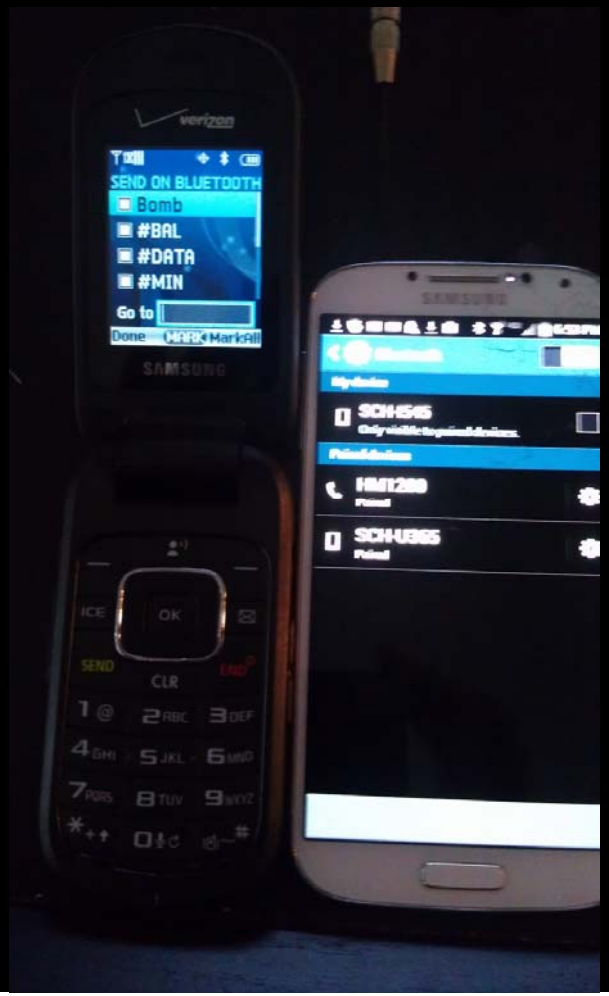
With attack platform loaded on the phone you have full control of all devices on the phone including TDOS, Brickmode etc.

Setting up ring tones as your specific payloads.

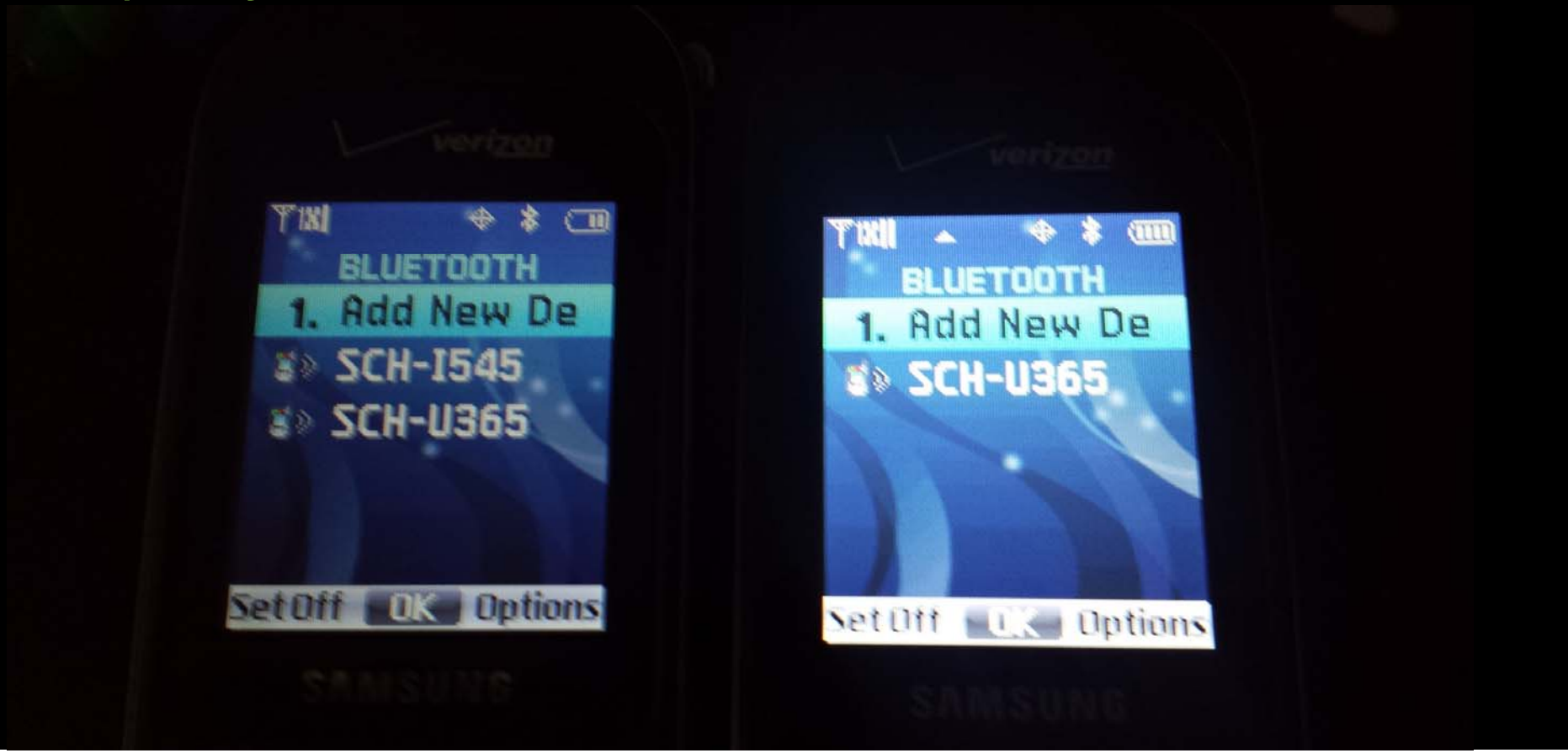
Setting ringtones will trigger the malformed ringtone processes on the events that trigger them.



CheeseBox?

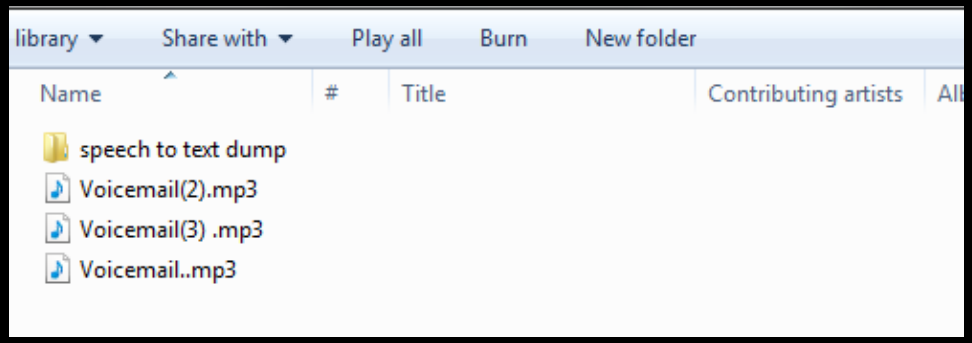

verizon
SEND ON BLUETOOTH
Bomb
#BAL
#DATA
#MIN
Go to
Done
Mark All
SAMSUNG
SCH-S45
SCH-U365
OK
CLR
SEND

Call one phone number. The call is passed off via Bluetooth to a second phone. The second phone calls your intended number creating a nearly untraceable phone proxy.

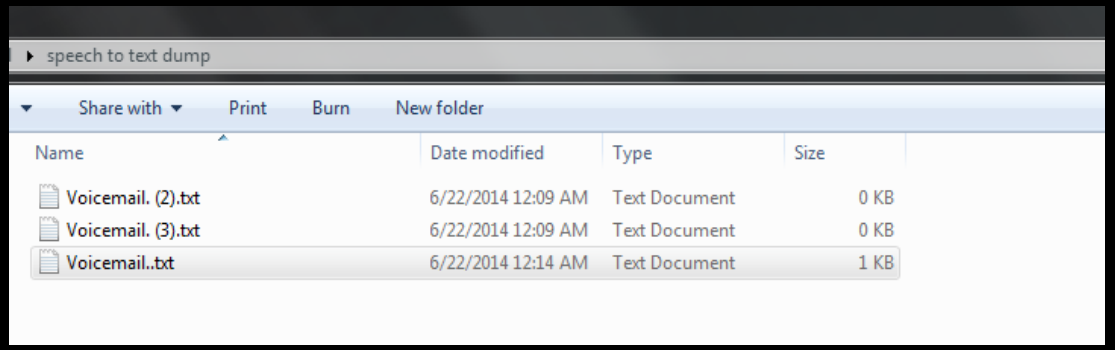


Weaponized Phone calls target number(s) 3 times in a row and records an MP3 to a Bluetooth connected PC the 3rd call that should go straight to voicemail.

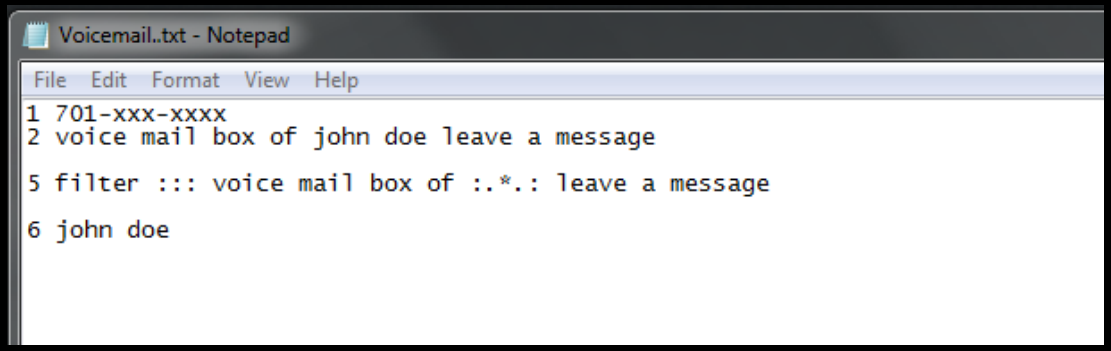
Files created with Bluetooth connection



Output of S2Text files



Run MP3 through speech to text open source software

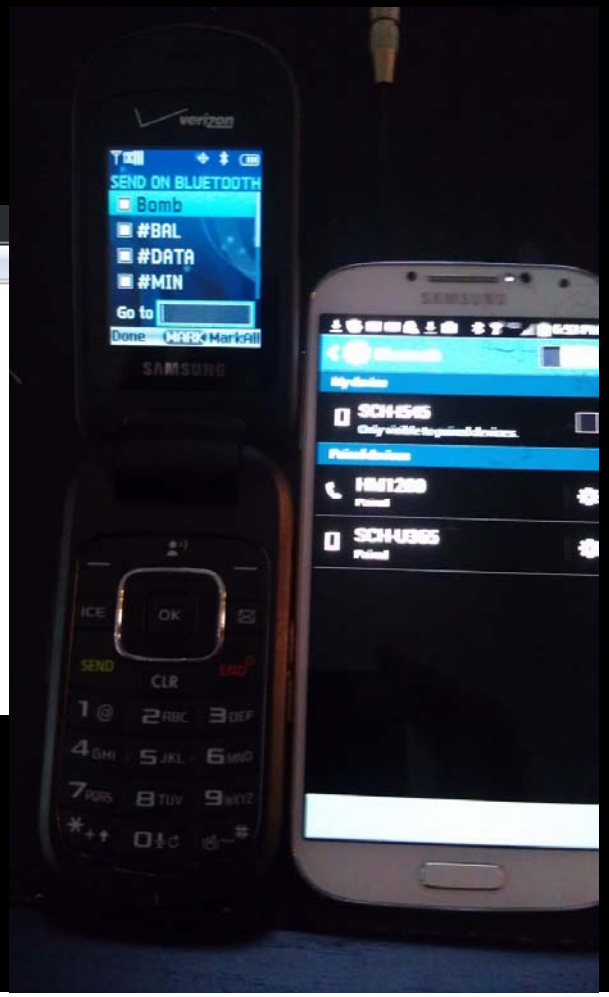


Phone script will call in and use the input information from the list to activate line of service.

Program bot.txt - Notepad

File Edit Format View Help

```
bt/0 #mac any 1-254


k1 #english
k3 #option k1 pre payed option # option k2 2 dollars a day you use it
if option k1 4342-xxxx-xxxx-xxxx 07/07 cvv512
k1
k1
k5 #5.*. # 90210 areacode for number
k1


call number range 701-xxx-xxxx/701-xxx-xxx call --3-- voicemail.mp3 (1-900)
```



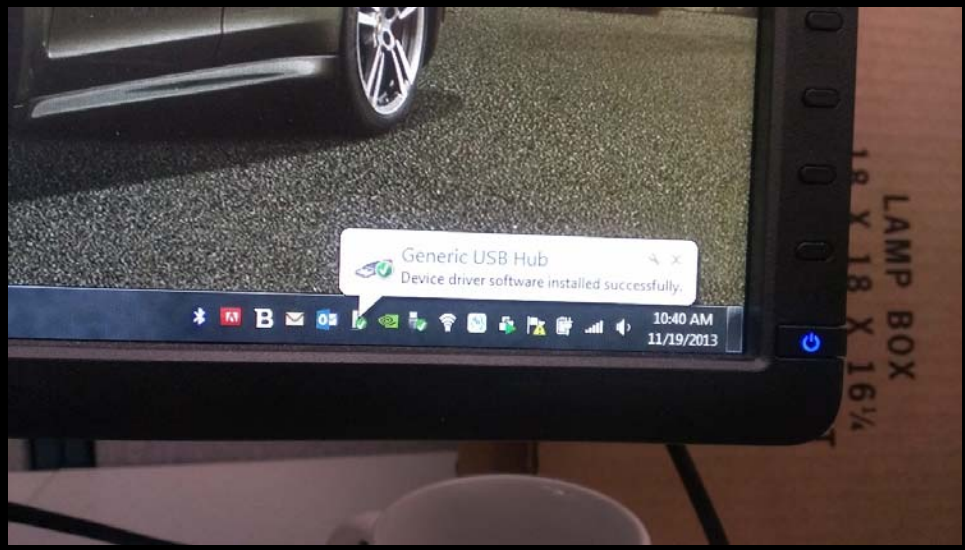
This Prepaid Cell Phone Can Deny Legitimate Phone Calls for 5 Days Straight

- Anonymous Purchase
- 2 Dollars Days That it is Used
- Untraceable Can be Charged With Solar USB Charger PRL List Hopping.
- Easily hidden inside light fixture at publicly accessible facility
- Total investment for a 5 day TDOS attack platform is $20 USD with Solar USB charger

Phone Being turned into CALLBOMBER

Firmware and PRL Being Updated

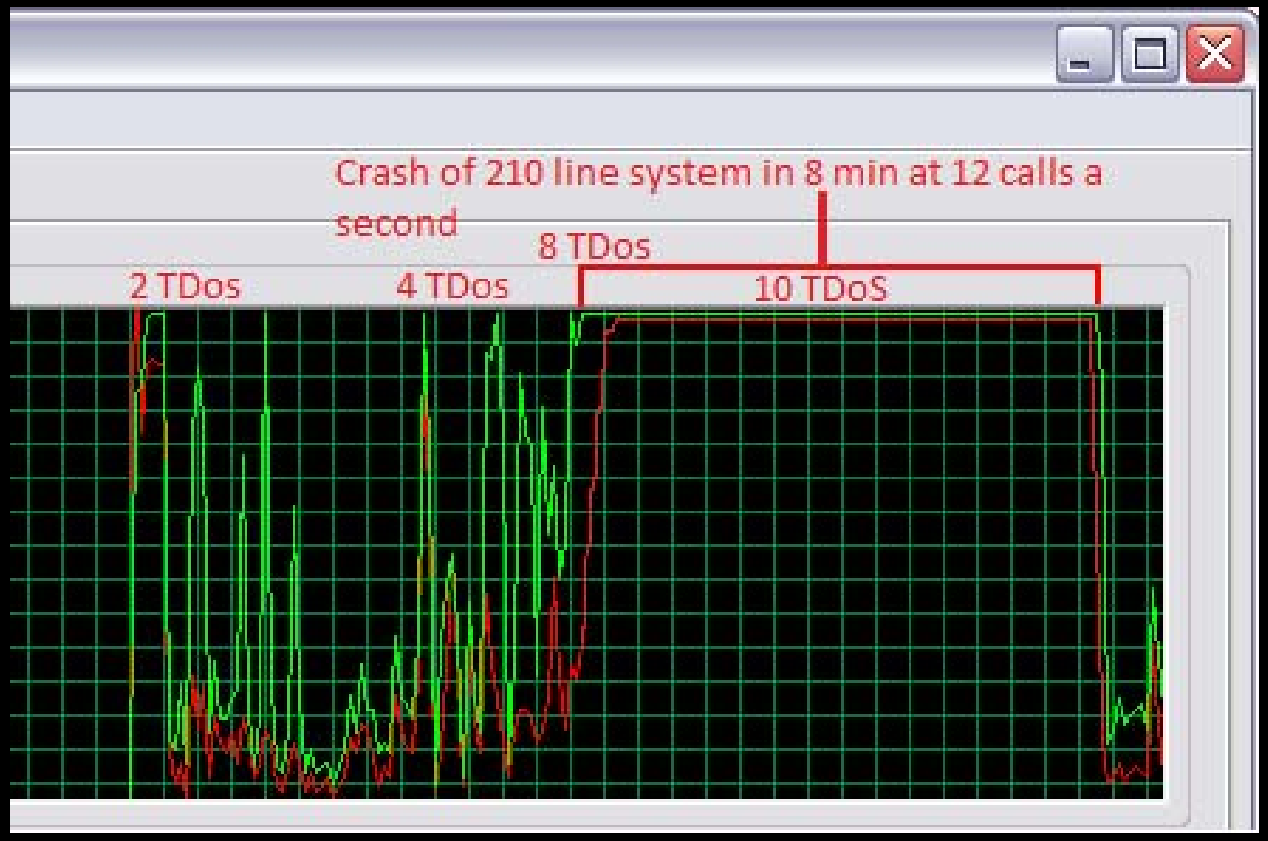
Plugged into Laptop and Re-flashed in under 8 min.



Crashing of call software by TDOS

Launching of 10 phones with weaponized platform

CPU and ram utilization crashes call center VM



Scenarios of TDOS

- Block 911 system
- Alarm companies for break ins
- Federal agencies during terrorist attack
- Stores during holiday seasons
- Any person or organization that is disliked

Thanks For Inviting Me and For Your Time
Any Questions Feel Free to Contact Me.

Special thanks to My Wife and family
The big guy in the sky for a cool name for computer security
Tim Help with schpelling on final eddit
Best Friend Scott
Hi Mom

Westonheckerdefcon@gmail.com
Westonhecker@twitter
Phone Number 701… Never Mind