

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 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, made enclosure for teensy 3.0 that looks like iPhone for Pen-testing, RFID Scanner that mounts under chair.
- About 9 years of REAL 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 I phones”.
- 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 I phones With Teensy 3.0



RFID Badge Reader Scans Through Seat Where Customers Wallet Would Be.



DDoS what is it TDoS What it is? 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.

Current methods of TDOS how it has evolved

- (SIP Trunk) SIP trunking is a Voice over Internet Protocol (VoIP) and streaming media service based on the Session Initiation Protocol (SIP) by which Internet telephony service providers (ITSPs) deliver telephone services and unified communications to customers equipped with SIP-based private branch exchange (IP-PBX) and Unified Communications facilities.
- (PRI) The Primary Rate Interface (PRI) is a standardized telecommunications service level within the Integrated Services Digital Network (ISDN) specification for carrying multiple DSo voice and data transmissions between a network and a user. line consists of 24 channels, 1 for Data caller ID information.
- In the wild there are a lot of TDOS in conjunction with credit card and bank fraud.

Current Methods of TDOS

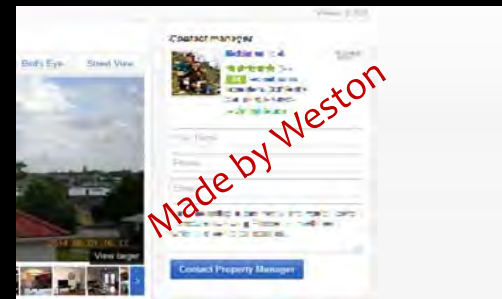
Caller ID Spoof Reflection Attack

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



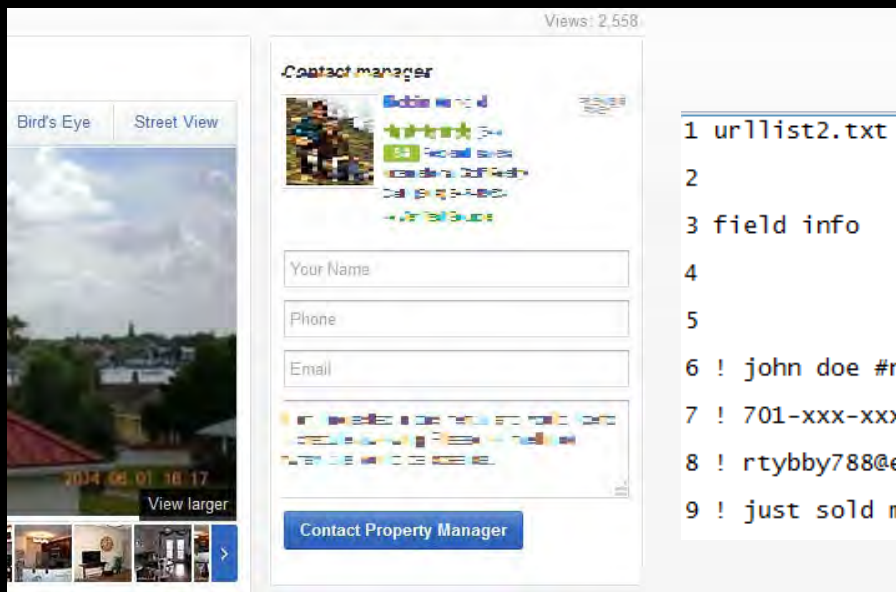
Thousands of calls returned to the number that they believe called them



Realtor pages use the same scripts for inquiries generation of a list.

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.

```
1 urllist2.txt
```

```
2
```

```
3 field info
```

```
4
```

```
5
```

```
6 ! john doe #name
```

```
7 ! 701-xxx-xxxx #phone
```

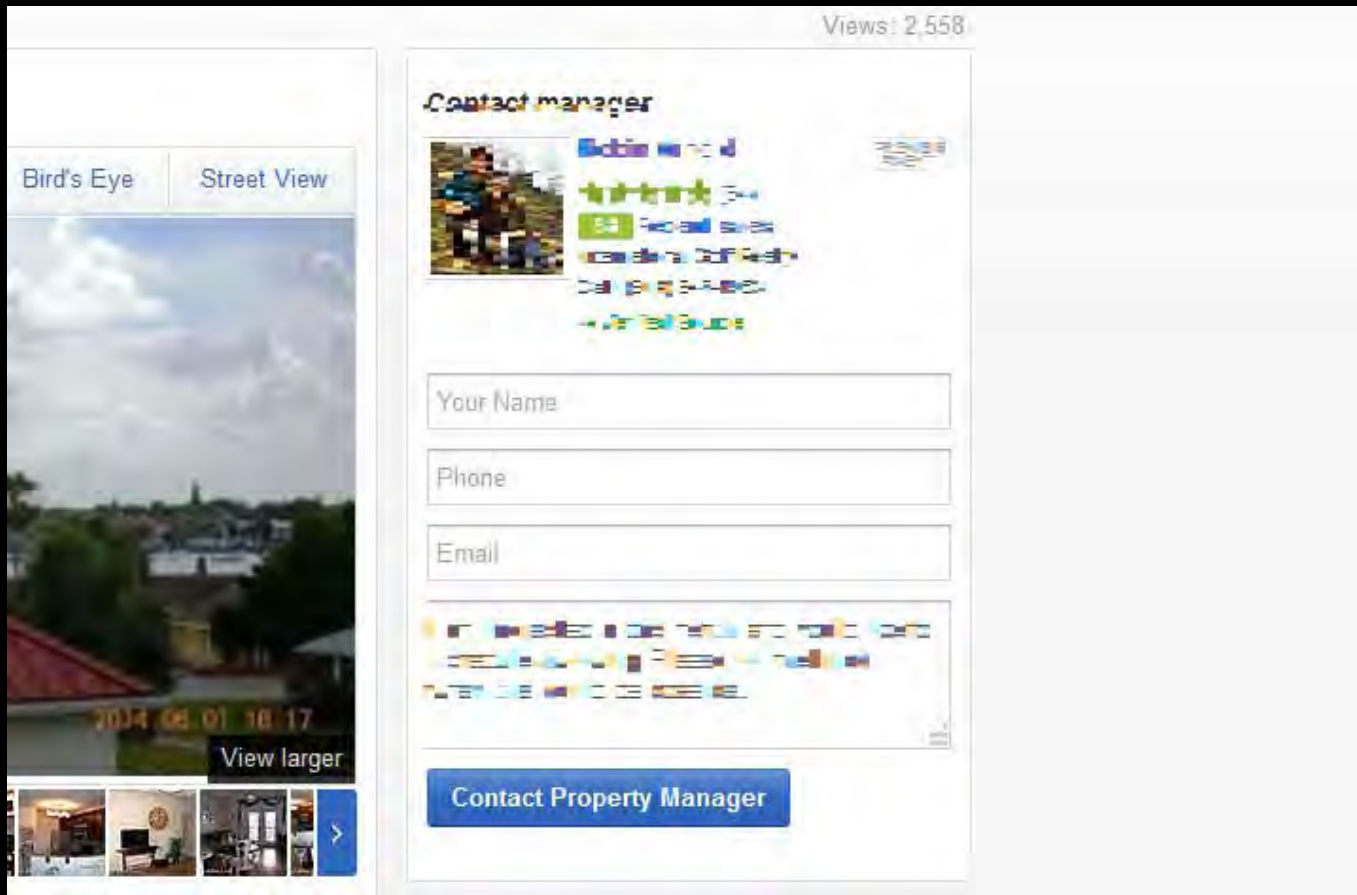
```
8 ! rtybby788@emaildomintest567.com #email
```

```
9 ! just sold my house in nevada looking at homes in the area please call#comment box
```

Web scripts 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.



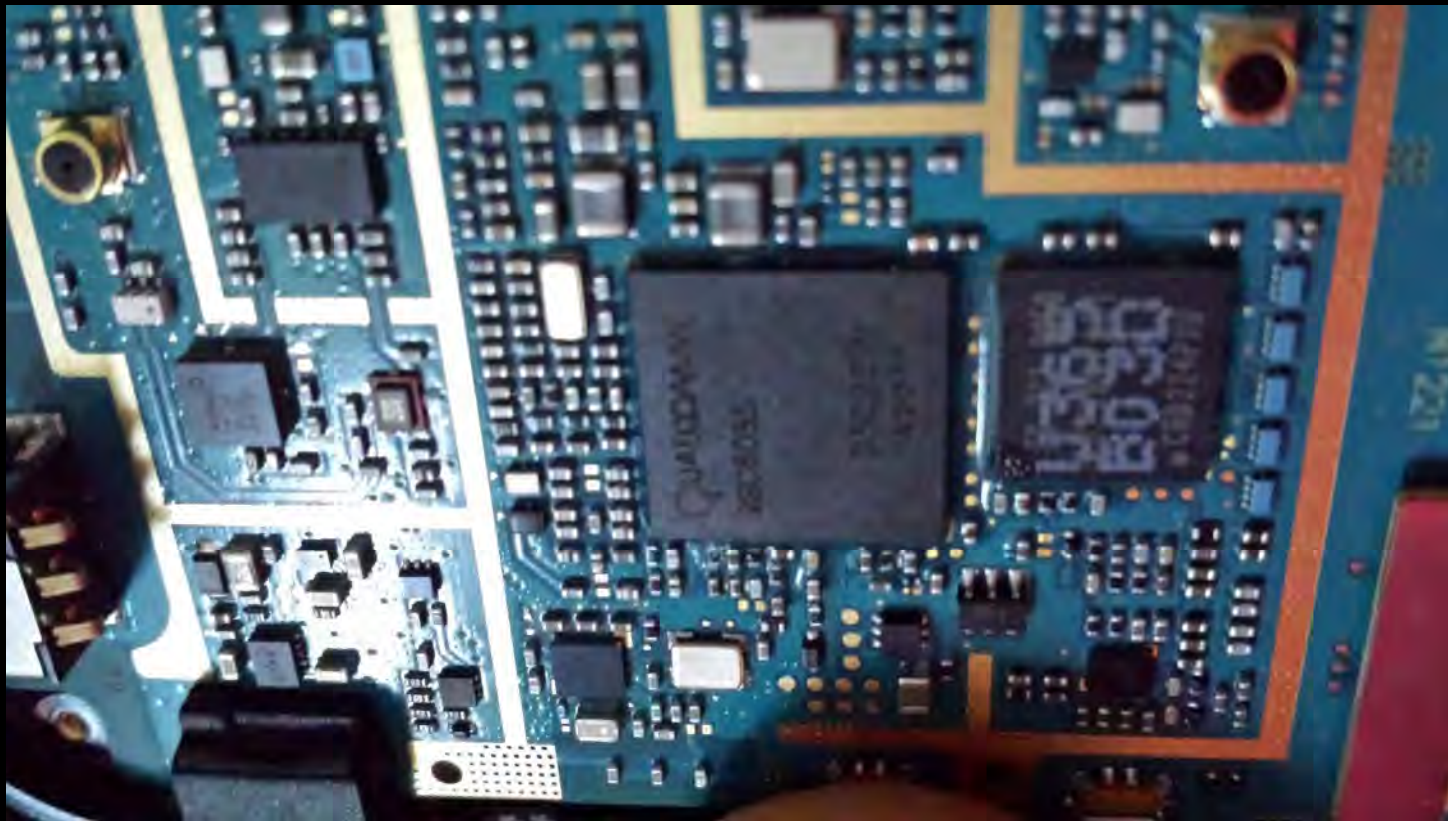
Explanation of how I developed a OEM/Weaponized cellphone platform



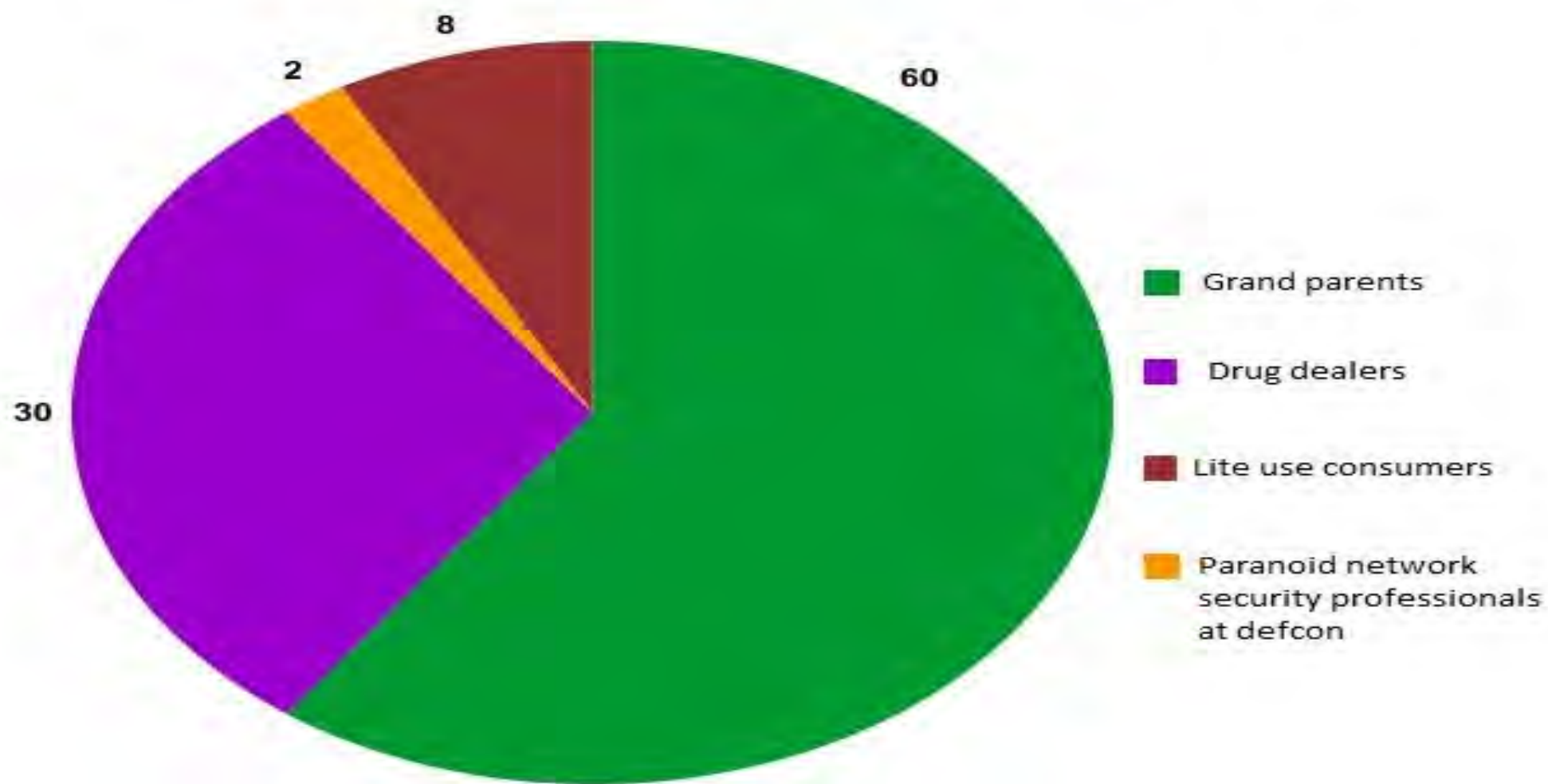
Prepaid Cell Phones Running Brew 3.1
Operating Systems CDMA 1X 800/1900 mHz
Digital Only Samsung U365 aka Gusto-2



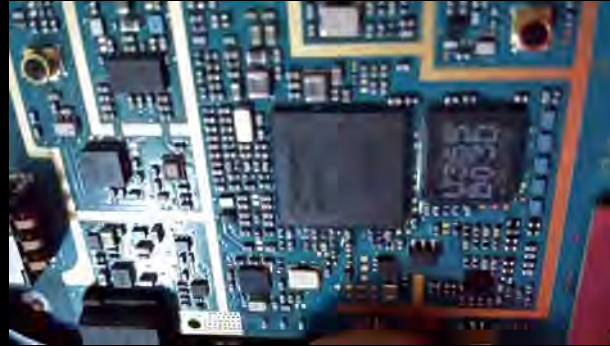
Qsc6055 192mhz processor, Weaponized platform
Works on all value tier qualcomm qsc60XX.



Pre Payed Phone Use Personal Study 2014



Qsc6055 192mhz processor, Comes with Secure Boot, SEE, SFS



The developer editions of these models support bootloader 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 bootloader, preventing these types of modifications. Until now

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

Written in C +



BREW provides the ability to control annunciators (typically located at the top of the display—RSSI, battery, voice mail, etc.); the activation or deactivation of annunciators by BREW applications. This capability shall be provided by default if the UI is runs on top of BREW. The OEM shall 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 ringtone

BREW provides the IRingerMgr interface that allows an OEM 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).

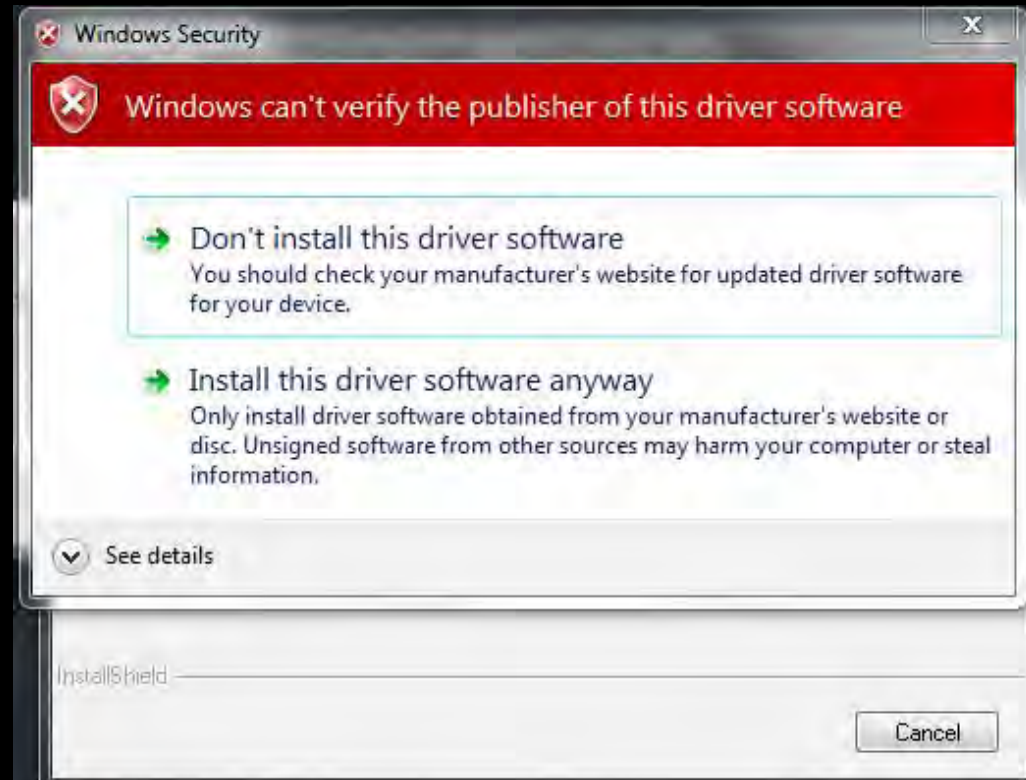
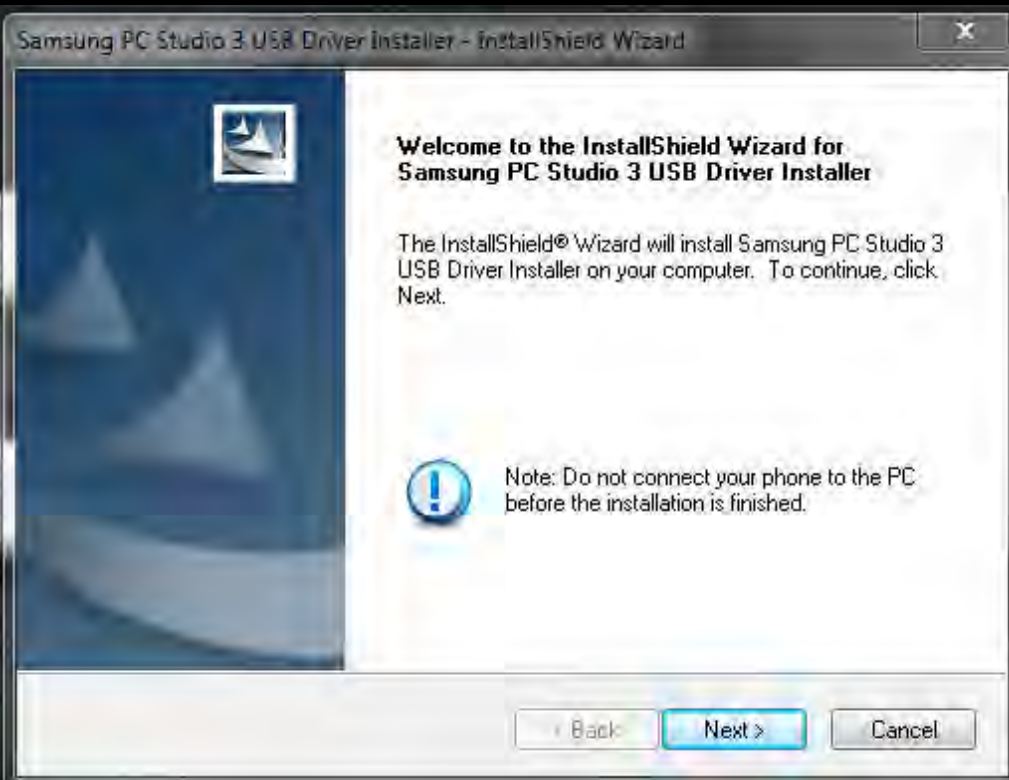


Clam-type phones refer to all handsets on which parts of the handset can be folded or rotated to cover the main LCD or the keypad. On these devices, some applications such as multimedia applications for example, may need to alter their functional use of hardware or services provided by the device depending upon events generated by the action of the user.

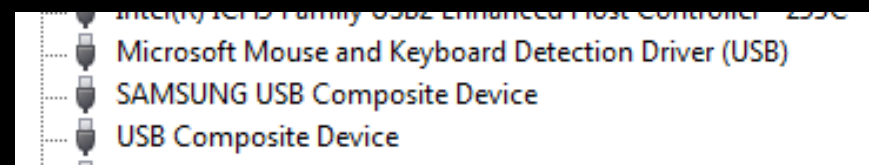
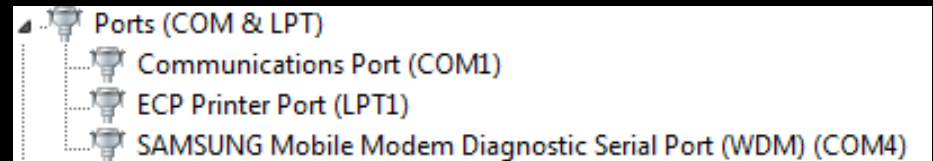
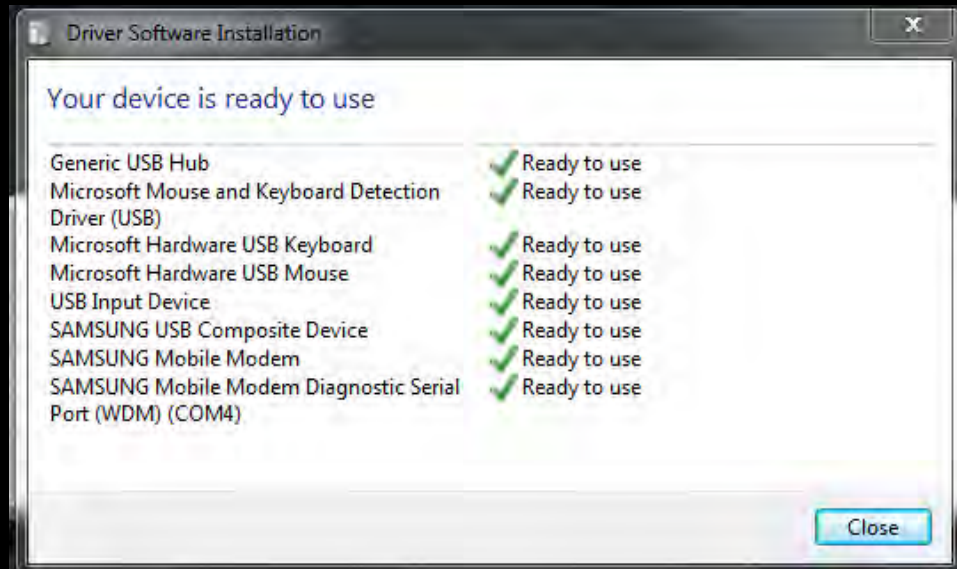
Secondary display: For devices supporting a secondary display, the display shall be made available to applications requiring display services when the clam is closed.



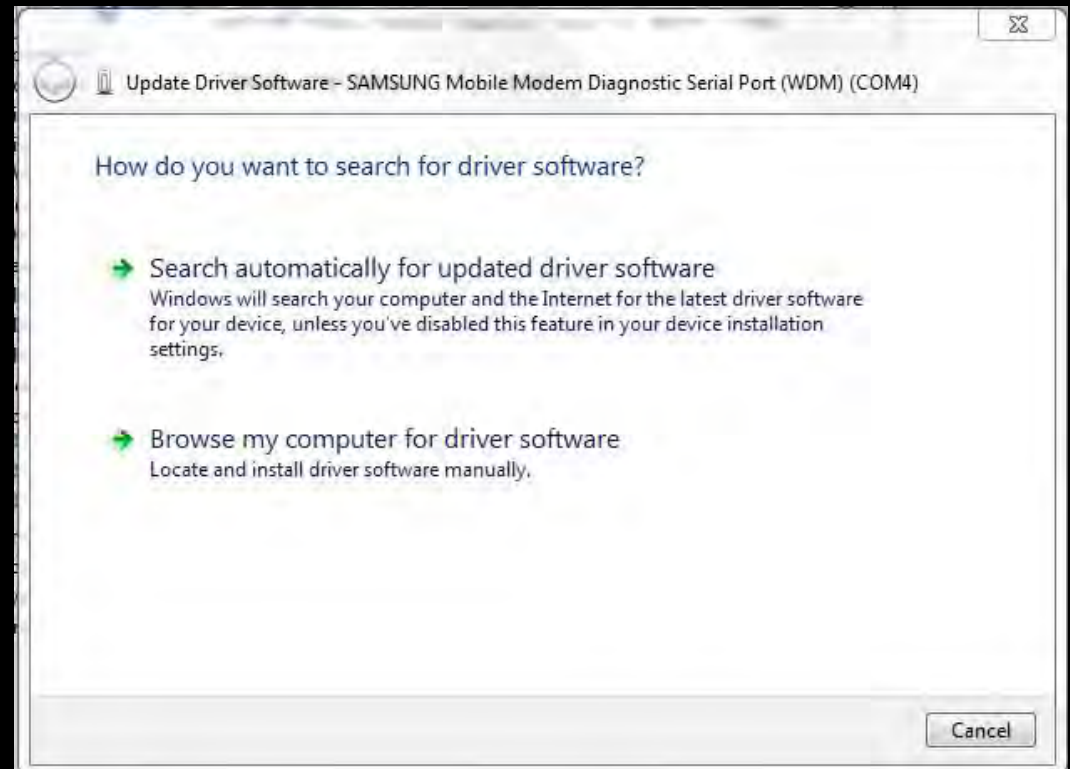
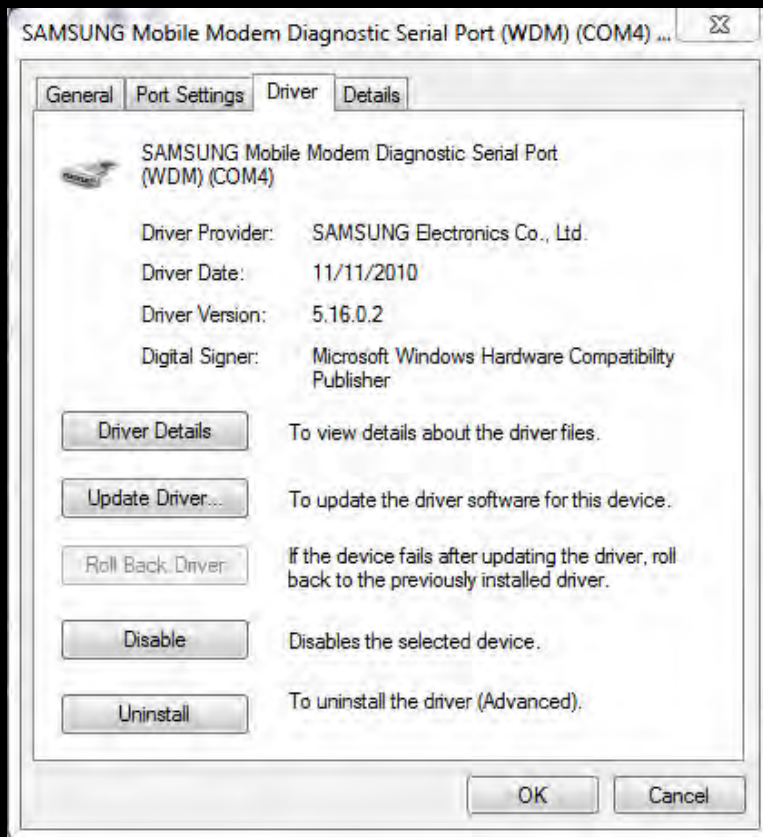
Modified executable allows for the software to be pushed to the device bypassing security feature easily using a loopholes with the certificate expiration process.



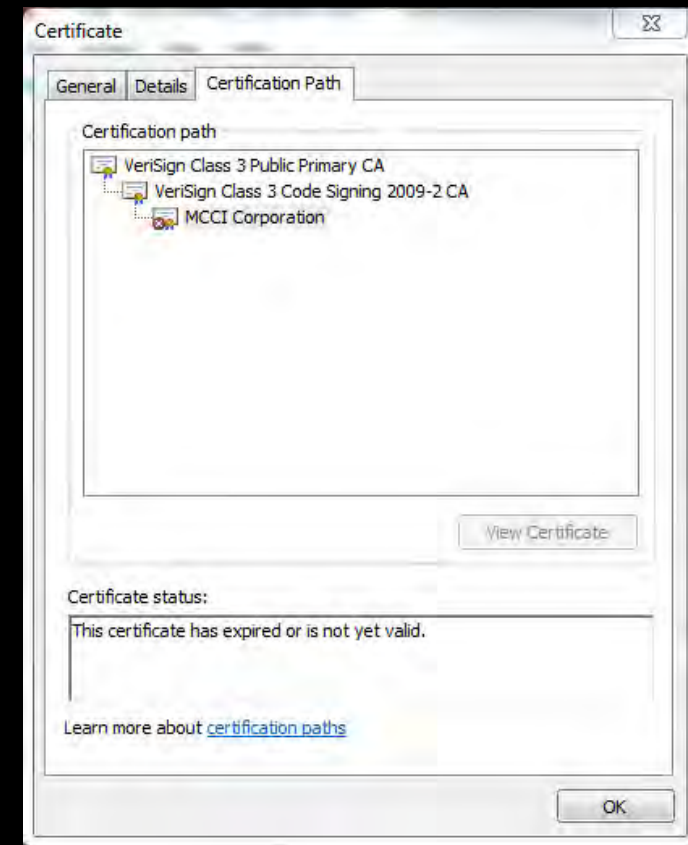
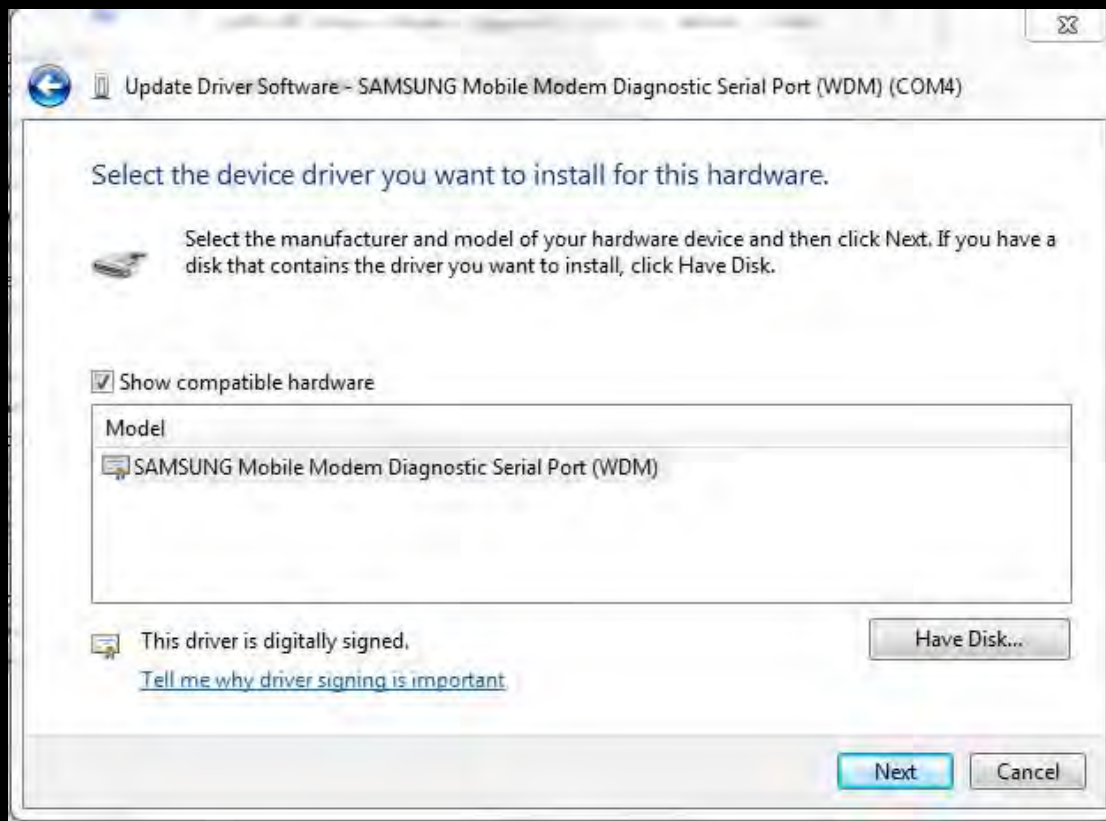
This error is exploited by running modified executable while other device is installed with a valid signed driver.



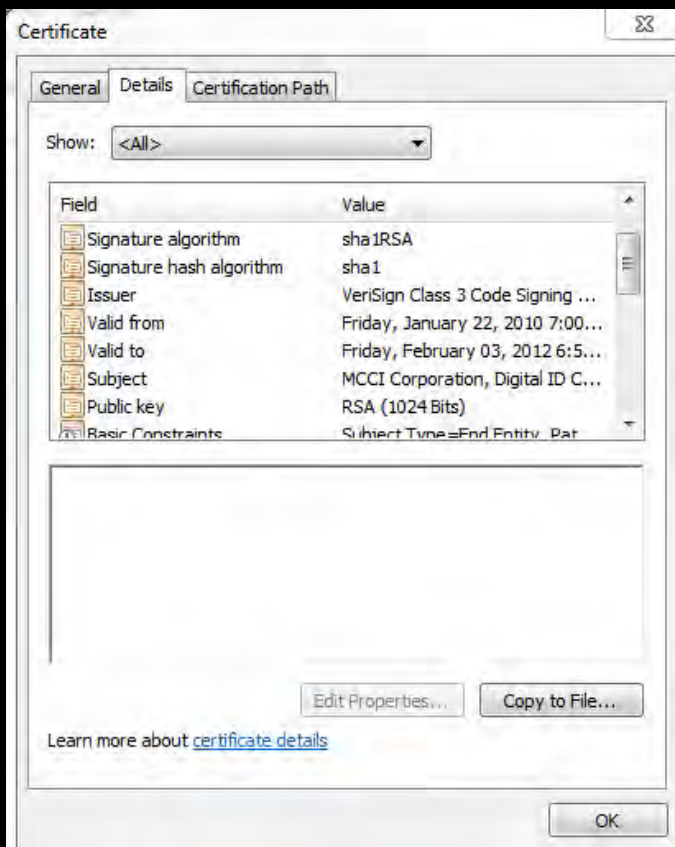
Once the driver is updated on the PC this allows full attack surface support.



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



Certificate expired in 2012 along with interaction with device to bypass security feature sets.

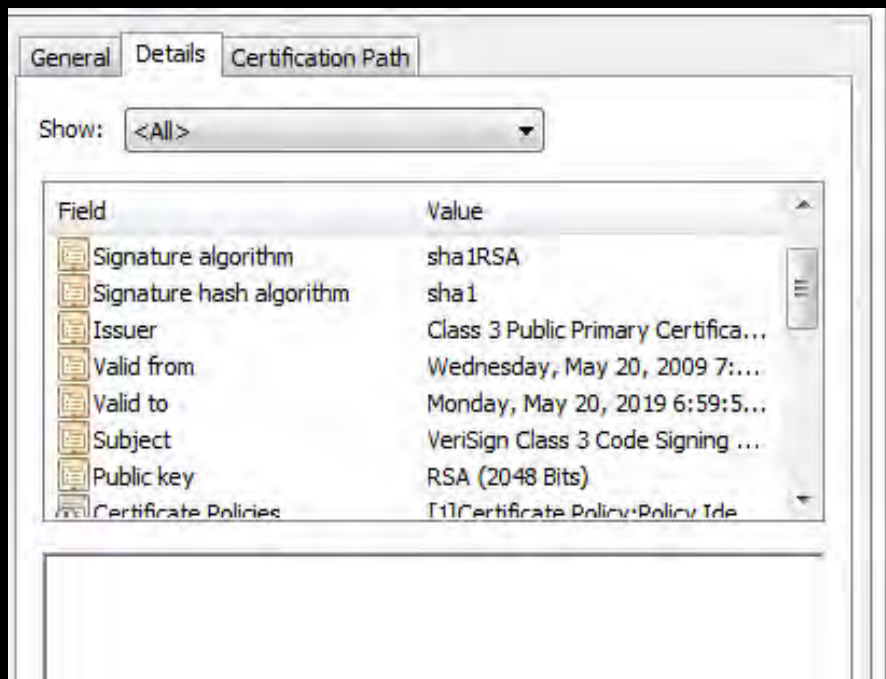


```
..Éu-, AAH<|* H% 3AAiiiiiiii, AiiiiiiiH%\$cH%t$+whfi H<ùH...Éu, Aé, 30Z-ŠËÿ+êš „Atqh'
MCCI(r) USB Communications Enumeration -- V5.16 build 2702 (Nov 10 2010 15:09:56)
```

```
C U S B D t i m e o u t I n M s e c      I n i t A c t i v i t y B u g C h e c k      I n i t A c t i v i t y B u g C h e c k
E n a b l e C U S B D t i m e o u t D b g      M C C I U S B _ c a l l U S B D      M C C I U S B _ g e t P o r t S t a t u s      M C C I U S B _ c a l l U S B
N T      G E T _ S T A T U S _ F R O M _ I N T E R F A C E      G E T _ S T A T U S _ F R O M _ D E V I C E      C L E A R _ F E A T U R E _ T O _ E N D P O I N T      C L E A R _ F E A T U R E
T   s p   || *   | d + | 4 q   ||   | s p   - | 2 - 0   |   | d   | T   1 4 q   | 2 q   | A + p   s   t   d   T   4 q   2 | a + D - A   |   | t   | d q   | T *   | 4 -   | 2 - A   |   | 4   R - p
A + p   "   " 4 s   " 2 0 a - 0 | A - p - | q P   |   | 4 *   | R - 0 | a - 0 s   A p s   s   P   ,   2 - 0   - |   - R - 0   s   t q   d s   T   4 s   r | a + D - A   "   " t *   " d +   " T q   " 4 s   " * A   s   t   d s   T s   4   R | a + D - A
```

```
ERROR
+CME ERROR:
+CMS ERROR:
CONNECT
CONNECT
BUSY
NO ANSWER
NO DIALTONE
NO CARRIER
>
```

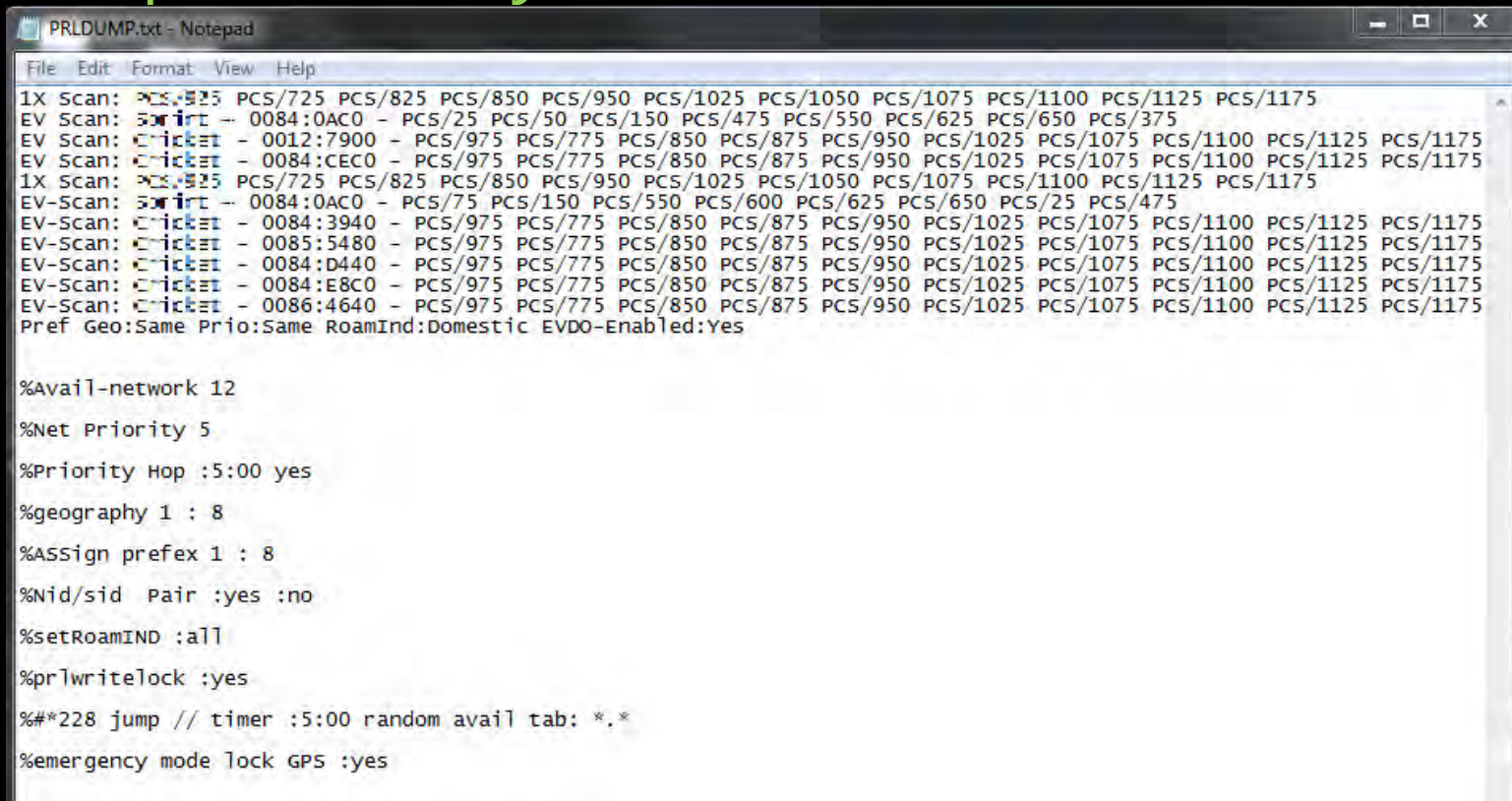
Modified driver files allow modifications of all device information.



Name	Date modified	Type	Size
hosts	6/14/2014 9:36 PM	File	1 KB
sscdcm.sys	11/11/2010 12:11 ...	SYS File	16 KB
sscdcmnt.sys	11/11/2010 12:11 ...	SYS File	16 KB
sscdserd.sys	11/11/2010 12:11 ...	SYS File	139 KB

Device Information	
Software:	SKACLZ43
Compiled:	Jul 15 2013 10:51:06
Released:	Aug 18 2011 U365.04
pESN:	0x80F6B2A2
MEID:	0xA0000045C38D09
IMEI:	
SCM:	0x2A
Bluetooth:	30:19:66:8B:E8:06
WiFi MAC:	
Number:	
User lock:	
PRL ver.:	53361
Protocol:	IS-2000 Rev 0 - (6)
Chipset:	Unknown (0x120FF0E1)
Build:	Q6055BSKACLZ439419
Model:	

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.



```
File Edit Format View Help
1X Scan: PCS/525 PCS/725 PCS/825 PCS/850 PCS/950 PCS/1025 PCS/1050 PCS/1075 PCS/1100 PCS/1125 PCS/1175
EV Scan: Sprint - 0084:0AC0 - PCS/25 PCS/50 PCS/150 PCS/475 PCS/550 PCS/625 PCS/650 PCS/375
EV Scan: Cicket - 0012:7900 - PCS/975 PCS/775 PCS/850 PCS/875 PCS/950 PCS/1025 PCS/1075 PCS/1100 PCS/1125 PCS/1175
EV Scan: Cicket - 0084:CEC0 - PCS/975 PCS/775 PCS/850 PCS/875 PCS/950 PCS/1025 PCS/1075 PCS/1100 PCS/1125 PCS/1175
1X Scan: PCS/525 PCS/725 PCS/825 PCS/850 PCS/950 PCS/1025 PCS/1050 PCS/1075 PCS/1100 PCS/1125 PCS/1175
EV-Scan: Sprint - 0084:0AC0 - PCS/75 PCS/150 PCS/550 PCS/600 PCS/625 PCS/650 PCS/25 PCS/475
EV-Scan: Cicket - 0084:3940 - PCS/975 PCS/775 PCS/850 PCS/875 PCS/950 PCS/1025 PCS/1075 PCS/1100 PCS/1125 PCS/1175
EV-Scan: Cicket - 0085:5480 - PCS/975 PCS/775 PCS/850 PCS/875 PCS/950 PCS/1025 PCS/1075 PCS/1100 PCS/1125 PCS/1175
EV-Scan: Cicket - 0084:D440 - PCS/975 PCS/775 PCS/850 PCS/875 PCS/950 PCS/1025 PCS/1075 PCS/1100 PCS/1125 PCS/1175
EV-Scan: Cicket - 0084:E8C0 - PCS/975 PCS/775 PCS/850 PCS/875 PCS/950 PCS/1025 PCS/1075 PCS/1100 PCS/1125 PCS/1175
EV-Scan: Cicket - 0086:4640 - PCS/975 PCS/775 PCS/850 PCS/875 PCS/950 PCS/1025 PCS/1075 PCS/1100 PCS/1125 PCS/1175
Pref Geo:Same Prio:Same RoamInd:Domestic EVDO-Enabled:Yes

%Avail-network 12
%Net Priority 5
%Priority Hop :5:00 yes
%geography 1 : 8
%ASSign prefix 1 : 8
%Nid/sid Pair :yes :no
%setRoamIND :all
%prlwriteLock :yes
%#*228 jump // timer :5:00 random avail tab: *.*
%emergency mode lock GPS :yes
```

Device development platform 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 with out having to load them on the device Effectively making it a development handset attack platform

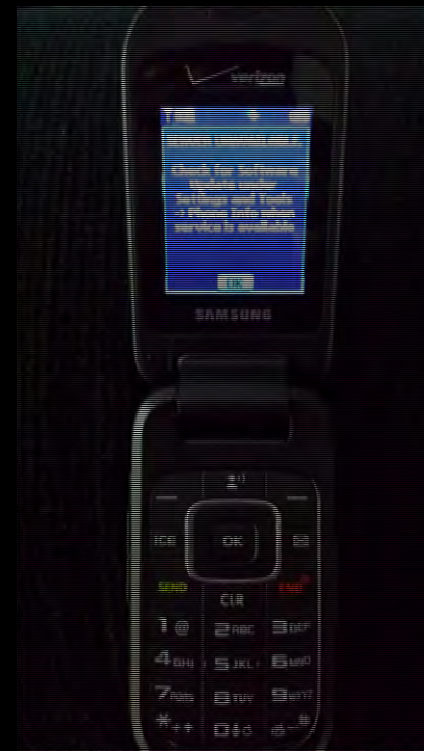


Now that you have your own fully unlocked platform what now...

OEM Development Platform



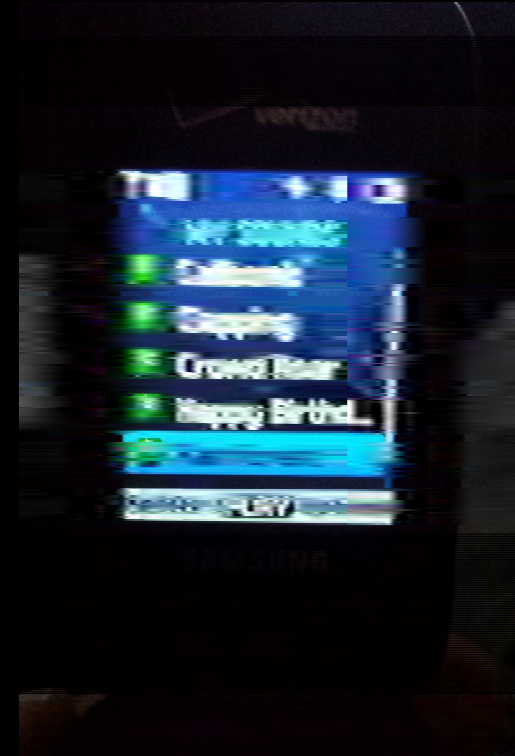
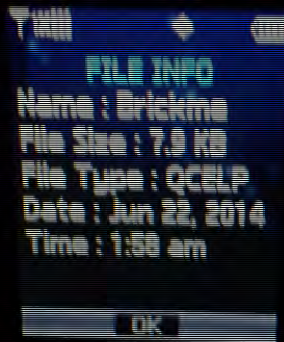
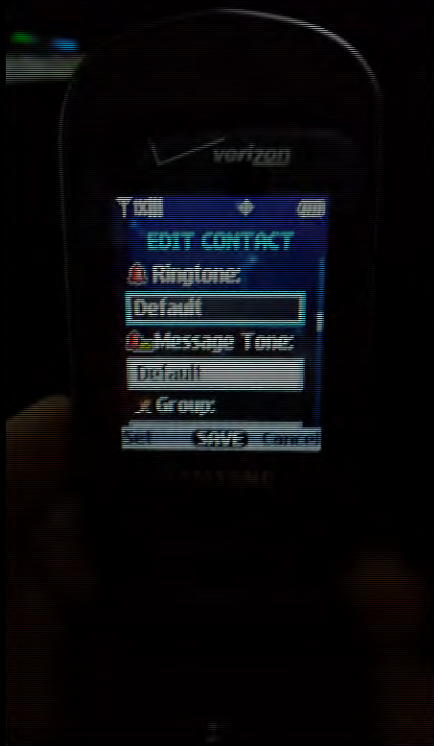
Weaponized Development Platform



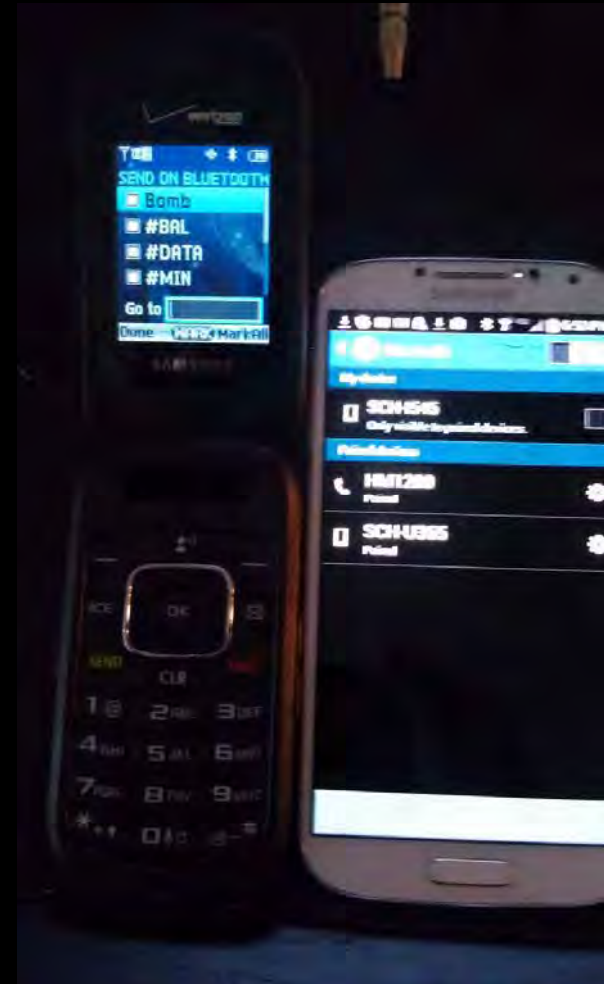
With attack platform loaded on the phone you have full control of all devices on the phone including TDOS, Brickmode etc.

Setting up ring tones as your specific payloads.

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



CheeseBox? History Evolution



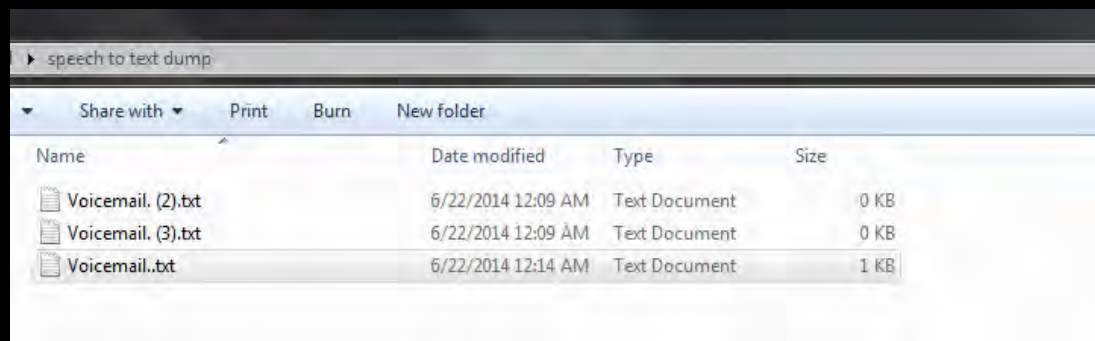
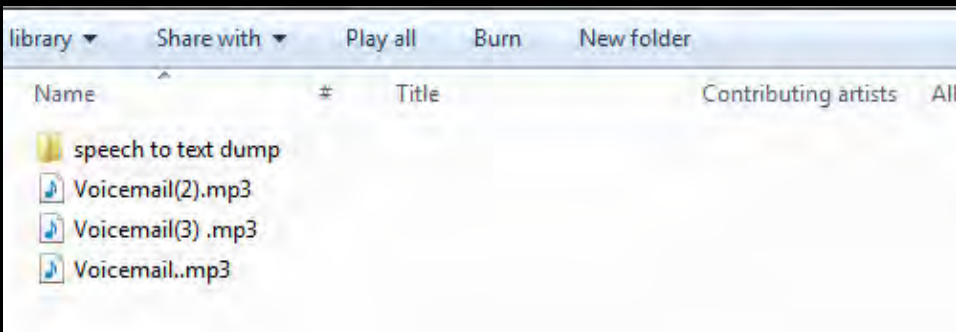
Call one phone number the call is passed off via Bluetooth to second phone calls your real number untraceable phone proxy



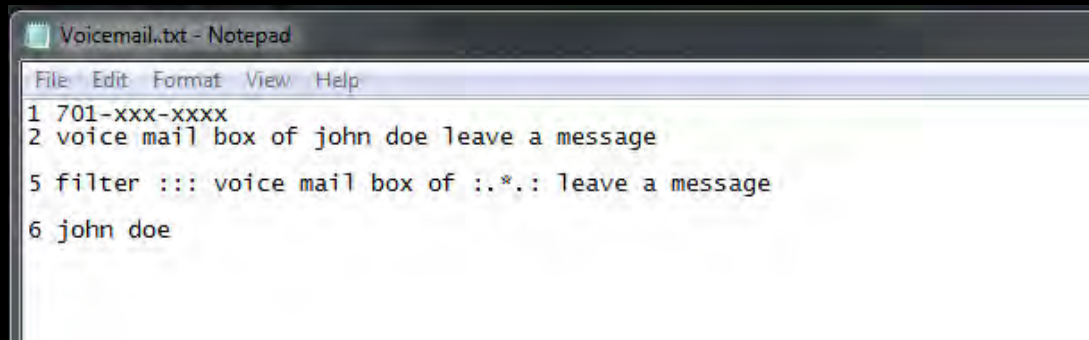
Bluetooth Connected Weaponized Phone calls 3 times in a row and records the 3rd call that is strait to voicemail to an MP3 on desktop

Files created with Bluetooth connection

Output of S2Text files



Run MP3 threw Speech to text OPEN source software



No need to call in to program phone
script will call in and use the input
information from the list below.

```
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 Strait

- Anonymous Purchase
- 2 Dollars Days That it is Used
- Untraceable Can be Charged With Solar USB Charger PRL List Hopping.
- GPS Not Recoverable Unless in 911 Mode which can easily be turned off if you flash phone before activation.



This kit shown here I built for 21 dollars total.

- Prepaid phone 16\$
- Solar USB charger 5\$
- 2 Dollars Days That it is Used
- Untraceable Can be Charged With Solar USB Charger PRL List Hopping.
- *228 bypassed to lock in PRL hop list and lock GPS statis .
- Stable non stop calling for 5 days strait
- Alarm sets phone to Brick on 5th day with malformed ringtone.

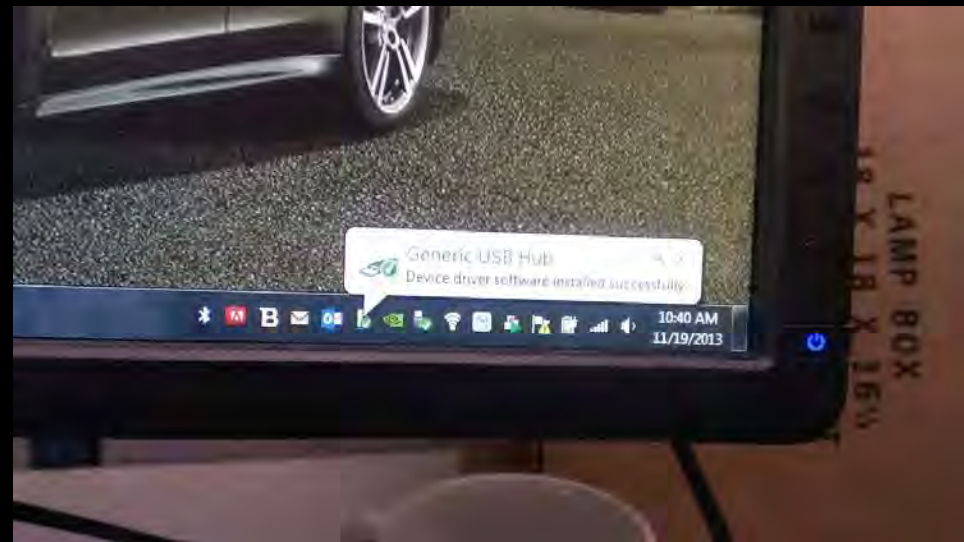


Phone Being turned into CALLBOMBER

Plugged into Computer Firmware and PRL Being Updated



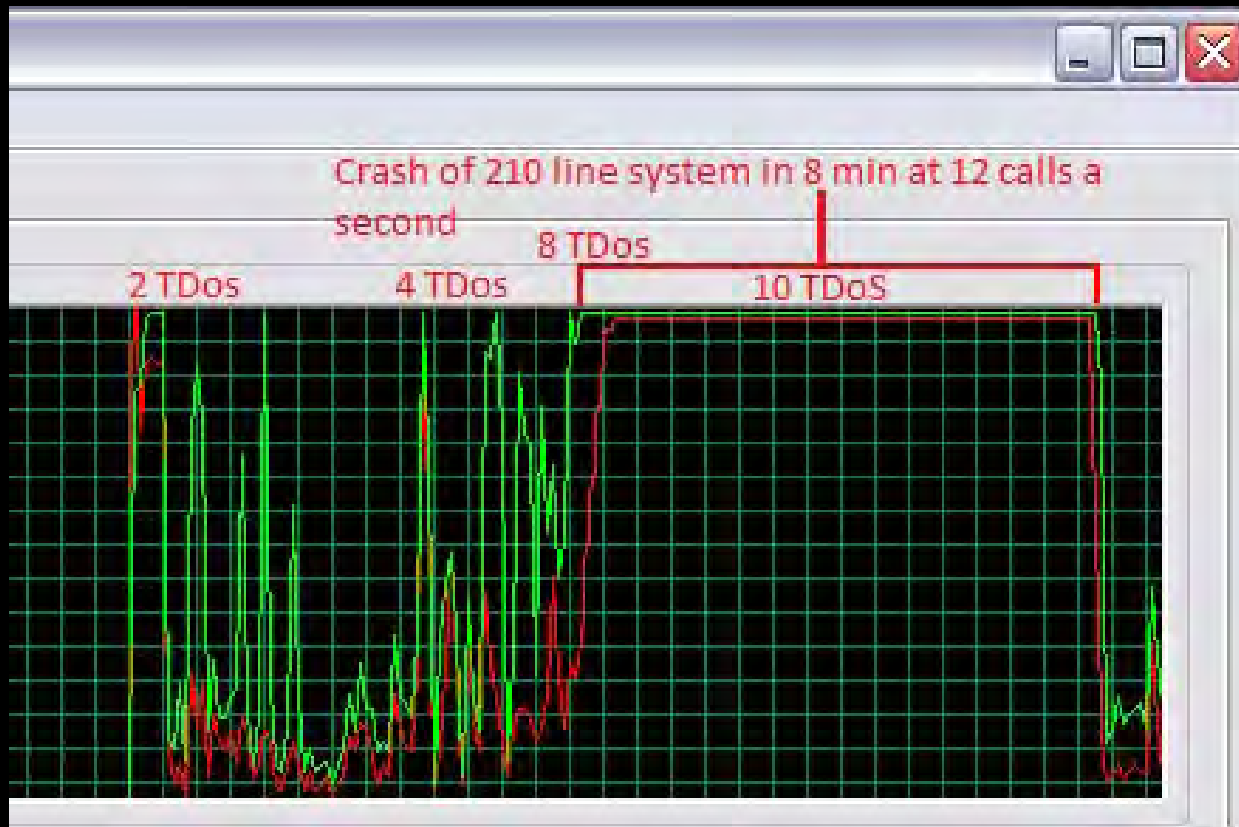
Plugged into Laptop and Re-flashed in under 8 min.



Crashing of call software by TDOS

Launching of 10 phones with
weaponized platform

CPU and ram utilization crashes call
center VM



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



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