Security Now! #438 - 01-14-14
NSA ANT: What We've Learned

Today on Security Now!

- Target's PoS PoS systems,
- A BAD and ultra-potent next-generation DDoS technology,
- News about the growing RSA security conference boycott,
- More on port 32764,
- A new security tool on Kickstarter,
- Net Neutrality takes it in the teeth... again...
- A quick survey of new and returning Sci-Fi on the tube...
- And WHAT WE'VE LEARNED about the NSA's capabilities.

Security News:

2nd Tuesday of the Month:

- Rather quiet this month.
- Only FOUR updates, none critical.
- Only some versions of windows and server and office.

XP's April 14th countdown...

- 83 days left!

ANOTHER "Target" Data Breach: 70 Million on TOP of the 40 Million!

- It was MALWARE installed on Target's Point-Of-Sale Terminals
    - 40 million cards, CVV numbers and encrypted PIN codes -- PLUS --
    - 70 million customer's PII (personally identifiable information).
    - http://www.scmagazine.com/target-ceo-confirms-malware-on-pos-machines-talks-chip-cards/article/329166/
- http://arstechnica.com/information-technology/2014/01/hackers-also-pilfered-personal-data-on-70-million-target-customers/
- First Breach: http://arstechnica.com/security/2013/12/secret-service-investigating-alleged-credit-card-breach-at-target/
- http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/
- http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=3
-

Neiman Marcus "brick and mortar" stores are also reporting trouble from mid-December.

- http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/

New Ultra-Strong DDoS floods generating 100 Gbps.

- DDoS & Bandwidth Amplification...
  - First: Simple SYN floods (1:1) -- packet rate and bandwidth
  - Then: TCP reflection (SYN/ACKs 4:1)
  - Then: DNS reflection (small query, large reply)
  - Now... NTP reflection
  - UDP port 123
  - "monlist" command: "get monlist" spoofing the victim's IP address.
    - Causes a list of the last 600 IP addresses which connected to the NTP server to be sent to the machine asking.
  - 234 byte "get monlist" command returns more than 48k of reply!
  - 6 IP addresses fit per packet... so 100 packets for 600 addresses!
  - Amplification factor 206x!
  - And *both* bandwidth amplification *and* packet rate amplification.

  - "monlist" command is enabled by default on older NTP servers.
  - US CERT recommends: disable the monlist command or upgrade to the latest version of NTP (v4.2.7p26) which disabled the entire monlist functionality.
  - Available since March 24th, 2010.

- http://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks
- https://www.us-cert.gov/ncas/alerts/TA14-013A

RSA Conference Boycotters surges to NINE
http://www.informationweek.com/security/vulnerabilities-and-threats/9-security-experts-boycott-rsa-conference/d/d-id/1113360?piddl_msgid=197414#msg_197414

The NSA has so much information that it cannot understand what it has.

- LAUSANNE, Switzerland—William Edward Binney:
- A former highly placed intelligence official with the NSA, resigned and turned whistleblower on Halloween of 2001... after 32 years with the agency, because: "could not stay once the NSA began purposefully violating the Constitution."
- Considered to be one of the best mathematicians and code breakers in NSA history.
- Creator of some of the computer code used by the National Security Agency to snoop on Internet traffic around the world, delivered an unusual message last September to an audience worried that the spy agency knows too much:
- He said: "The NSA knows so much that it can't understand what it has."
  - http://www.businessinsider.com/nsa-whistleblower-william-binney-was-right-2013-6

Obama administration to announce new NSA guidelines Friday.

- Widely expected to change the way cell phone metadata is collected & managed.
    - Hopefully... the providers will keep it and reply to specific requests.
    - From the NSA's perspective, having all that data is an intuitively COOL capability... but somewhat surprisingly, there's been ZERO evidence that it's been of any practical value whatsoever.

What It's Like When The FBI Asks You To Backdoor Your Software

- http://securitywatch.pcmag.com/security/319544-what-it-s-like-when-the-fbi-asks-you-to-backdoor-your-software
- Max Eddy, Jan 8th, 2014
- <quote> At a recent RSA Security Conference, Nico Sell was on stage announcing that her company—Wickr—was making drastic changes to ensure its users' security. She said that the company would switch from RSA encryption to elliptic curve encryption, and that the service wouldn't have a backdoor for anyone.

- As she left the stage, before she'd even had a chance to take her microphone off, a man approached her and introduced himself as an agent with the Federal Bureau of Investigation. He then proceeded to "casually" ask if she'd be willing to install a backdoor into Wickr that would allow the FBI to retrieve information.

- "A Common Practice"
  This encounter, and the agent's casual demeanor, is apparently business as usual as intelligence and law enforcement agencies seek to gain greater access into protected communication systems. Since her encounter with the agent at RSA, Sell says it's a story she's heard again and again. "It sounds like that's how they do it now," she told SecurityWatch. "Always casual, testing, because most people would say yes."

- [SNIP] <quote>
  It was clear that the FBI agent didn't know who he was dealing with, because Sell did not back down. Instead, she lectured him on topics ranging from the First and Fourth Amendments to the Constitution, to George Washington's creation of a Post Office in the US. [Nico said:] "My ancestor was a drummer boy under [George] Washington. Washington thought it was very important to have freedom of information and private correspondence without government surveillance."

GSM digital cell phone encryption was crippled from the beginning.

- Its designers wanted 128 bit keys.
- The British government wanted to be able to crack it for surveillance.
- West Germany wanted strong keys to keep East Germany from snooping
- After much back and forth, the key length was first cut in half, to 64 bits.
- ... then under British pressure, the last ten bits were all set to '0', rendering an effective key length of 54 bits.
- http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html#.Us_y_Edbx28.twitter

Port 32764 Router Backdoor Follow-Up:

- This is SO BAD that I created a bit.ly shortcut to scan a port:
  - http://bit.ly/port32764
- **13 (partially) reverse engineered backdoor commands**
  - 1: (Dump Config) HTTP admin username & password *and* WiFi (PSK) pre-shared key password!
  - 2: Get Config Var
  - 3: Set Config Var
  - 4: Commit NVRAM
  - 5: Set Bridge Mode ON.
  - 6: Show measured Internet speed.
  - 7: "Cmd" -- yep, a full command shell.
  - 8: Write File
  - 9: Return version
  - 10: Return modem router IP.
  - 11: Restore Default NVRAM... turns WAN admin back on!
  - 12 : Read some blocks (unsure)
  - 13: Dump NVRAM on disk and commit.

  - Cisco to issue firmware update by end of the month: "An attacker could exploit this vulnerability by accessing the affected device from the LAN-side interface and issuing arbitrary commands in the underlying operating system," Cisco said in an advisory published Friday. "An exploit could allow the attacker to access user credentials for the administrator account of the device, and read the device configuration. The exploit can also allow the attacker to issue arbitrary commands on the device with escalated privileges."

Net Neutrality takes it in the teeth.

- D.C. Court of Appeals:
- The court says ISPs have the inherent right to carry the traffic they choose, and that consumers can vote with their wallets to choose the ISP that provides the services they want.
- http://bgr.com/2014/01/14/net-neutrality-court-ruling/
- ***But... hopefully it was only that the FCC asked wrong!***
- http://www.techdirt.com/articles/20140114/08521425868/as-expected-court-strikes-down-fccs-net-neutrality-rules-now-what.shtml

"Techie Bonus" for our Show Note Readers: *Cloudflare's Nick Sullivan explains:*

- How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer
- http://blog.cloudflare.com/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer
- And Nick's "A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography"
- http://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography

Kickstarter:

- Universal Bootable Windows Password Reset Key:
- http://kck.st/1lFRZrX
- Google "password reset key" (currently 2nd link in results.)

Boob Tube Update:

- *Intelligence* (CBS): Why does an augmented top field combat operative require a sexy hot ex-Secret Service agent "to keep him alive"?? That's just dumb. It should have been a hot & sexy computer tech to reboot him if needed!
- *Almost Human* (Fox) - Never takes itself too seriously.
- *Helix* (SyFy) - Took itself WAY too seriously. So chock full of poor direction and ridiculous motivations that it was impossible to suspend disbelief.
- *Stargate SG1* - Truly a classic: A terrific premise for Sci-Fi
- *True Detective* (HBO) - Reminiscent of "The Killing"
- *Justified* (Showtime) - "Kicking ass" with the best of them.

Miscellany:

- TSA PRE ... is a WIN!!!!
- A pre-9/11 time machine.
- My experience

SQRL R&D Update:

- Data storage format stabilized.
- Been benchmarking SCrypt -- Colin Percival / Tarsnap

SpinRite:

Date: Saturday, 21 Dec 2013 19:14:21 -0000
From: "Ron Kurr" in Auburn, NH
Subject: Spinrite + VirtualBox + USB drive = data loss prevention goodness

Steve, I've stumbled upon something that I think others might be interested in but I wanted you to clarify something first. A little context seems appropriate. I'm a Linux weenie and noticed that most of the directions for getting Spinrite to operate within VirtualBox were all Windows based. Having an hour to spare I decided to try and get Spinrite to run under VirtualBox on my Linux i7. In a nutshell, Linux makes it much easier to do than Windows does and I was able to run several Spinrite virtual machines concurrently as I did real work. As an experiment, I tried using the Spinrite/VirtualBox combination with some of the USB hard drives I carry with me to and from work. Normally, Spinrite doesn't see the drives so I could never exercise the disks like you recommend but the Sprinrite/VirtualBox combination saw it like any other hard drive.

Here is my question: is Spinrite able to use the same deep scanning techniques with a virtualized USB drive like it does with a standard SATA drive? I know in the past you have recommended that people extract their USB drives from the enclosures and attach them directly to their

motherboard's drive controller so Spinrite can perform its deepest scans. Does VirtualBox's drive controller emulation actually allow Spinrite to treat the USB drive as if it were a native SATA drive or is the emulation just 'tricking' Spinrite into thinking that it is doing a deep level scan when, in fact, it is not. I'm very curious to hear your thoughts.

Thanks, Ron Kurr

NSA ANT: What We've Learned

Definitions:

- Interdiction - physical access
- An "Implant" - something "implanted" into another device
- Persistence - survives reboots, OS upgrades, etc.
- "PBD" - Persistent Backdoor
- "DNT Payload" - Digital Network Technologies

Both major "Big Iron" Internet router companies **Cisco** and **Juniper Networks** appear to be completely compromised… though perhaps not remotely.

- How do Cisco & Juniper react to this?
- How do their major customers?

"BananaGlee"

A software exploit made by Digital Network Technologies (DNT) for Juniper Netscreen ns5xt, ns50, ns200, ns500, ISG 1000, ssg140, ssg5, ssg20, SSG 320M, SSG 350M, SSG 520, SSG 550, SSG 520M, SSG 550M firewalls. Also works on Cisco PIX 500 series and ASA 5505, 5510, 5520, 5540, and 5550 series firewalls. Used for exfiltrating data from target networks.

"JetPlow":

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been widely deployed. Current availability restricted based on OS version (inquire for details). **Unit Cost:** $0

If the NSA can do this remotely, so can ANY other agency, government or hacker.

"SouffleTrough":

(TS//SI//REL) SOUFFLETROUGH is a BIOS persistence implant for Juniper SSG 500 and SSG 300 series firewalls. It persists DNT's BANANAGLEE software implant. SOUFFLETROUGH also has an advanced persistent back-door capability.

(TS//SI//REL) SOUFFLETROUGH is a BIOS persistence implant for Juniper SSG 500 and SSG 300 series firewalls {320M, 350M, 520, 550, 520M, 550M}. It persists DNT's BANANAGLEE software implant and modifies the Juniper firewall's operating system (ScreenOS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. It takes advantage of Intel's System Management Mode for enhanced reliability and covertness. The PBD is also able to beacon home, and is fully configurable.

(TS//SI//REL) A typical SOUFFLETROUGH deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. SOUFFLETROUGH is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been deployed. There are no availability restrictions preventing ongoing deployments. **Unit Cost:** $0

Huawei Technologies Co. Ltd.
A Chinese multinational networking and telecommunications equipment and services company headquartered in Shenzhen, Guangdong.

"HeadWater" appears to install 100% remotely:

(TS//SI//REL) HEADWATER is a Persistent Backdoor (PBD) software implant for selected Huawei routers. The implant will enable covert functions to be remotely executed within the router via an Internet connection.

(TS//SI//REL) HEADWATER PBD implant will be transferred remotely over the Internet to the selected target router by Remote Operations Center (ROC) personnel. After the transfer process is complete, the PBD will be installed in the router's boot ROM via an upgrade command. The PBD will then be activated after a system reboot. Once activated, the ROC operators will be able to use DNT's HAMMERMILL Insertion Tool (HIT) to control the PBD as it captures and examines all IP packets passing through the host router.

(TS//SI//REL) HEADWATER is the cover term for the PBD for Huawei Technologies routers. PBD has been adopted for use in the joint NSA/CIA effort to exploit Huawei network equipment. (The cover name for this joint project is TURBOPANDA.)

Status: (U//FOUO) On the shelf ready for deployment.

"SchoolMontana" - for Juniper J-series routers
"SierraMontana" - for Juniper M-series routers
"StuccoMontana" - for Juniper T-series routers

(TS//SI//REL) STUCCOMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

(TS//SI//REL) Currently, the intended DNT Implant to persist is VALIDATOR, which must be run as a user process on the target operating system. The vector of attack is the modification of the target's BIOS. The modification will add the necessary software to the BIOS and modify its software to execute the STUCCOMONTANA implant at the end of its native System Management Mode (SMM) handler.

(TS//SI//REL) STUCCOMONTANA must support all modern versions of JUNOS, which is a version of FreeBSD customized by Juniper. Upon system boot, the JUNOS operating system is modified in memory to run the implant, and provide persistent kernel modifications to support implant execution.

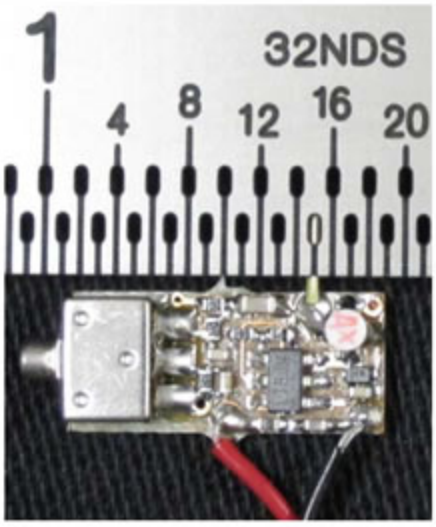
(TS//SI//REL) STUCCOMONTANA is the cover term for the persistence technique to deploy a DNT implant to Juniper T-Series routers.

“LoudAuto”:

(TS//SI//REL TO USA,FVEY) Audio-based RF retro-reflector. Provides room audio from targeted space using radar and basic post-processing.

(U) Capabilities

(TS//SI//REL TO USA,FVEY) LOUDAUTO's current design maximizes the gain of the microphone. This makes it extremely useful for picking up room audio. It can pick up speech at a standard, office volume from over 20' away. (NOTE: Concealments may reduce this distance.) It uses very little power (~15 uA at 3.0 VDC), so little, in fact, that battery self-discharge is more of an issue for serviceable lifetime than the power draw from this unit. The simplicity of the design allows the form factor to be tailored for specific operational requirements. All components at COTS and so are non-attributable to NSA.



(U) Concept of Operation

TS//SI//REL TO USA,FVEY) Room audio is picked up by the microphone and converted into an analog electrical signal. This signal is used to pulse position modulate (PPM) a square wave signal running at a pre-set frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal from a nearby radar unit, the illuminating signal is amplitude-modulated with the PPM square wave. This signal is re-radiated, where it is picked up by the radar, then processed to recover the room audio. Processing is currently performed by COTS equipment with FM demodulation capability (Rohde & Schwarz FSH-series portable spectrum analyzers, etc.) LOUDAUTO is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

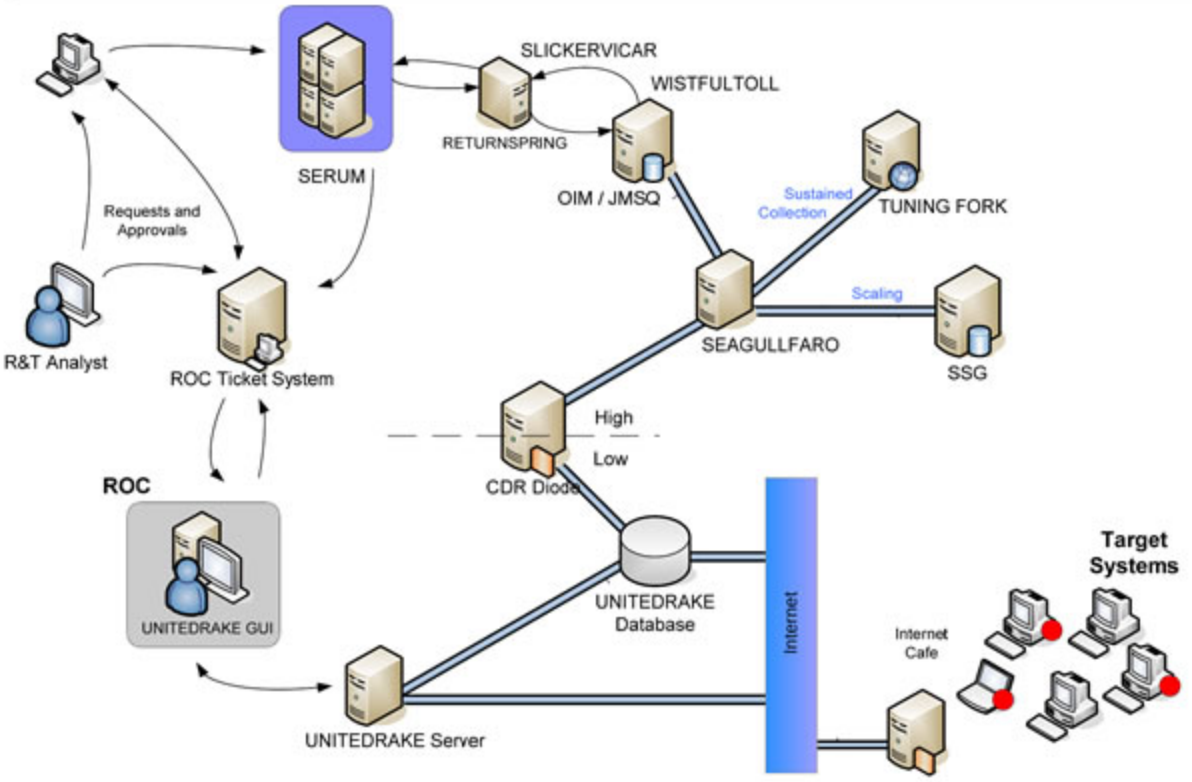
Unit Cost: $30

CTX4000 or PhotoAnglo are continuous wave (CW) (unmodulated) 1-4 Ghz radar transmitters. They passively illuminate a target, receive the re-radiated signal, mix it down (heterodyne) to eliminate the high-frequency radar, recover the signal, and export it to analysis.

“NightWatch” is a shielded computer which can recover, decode and display a video signal obtained from the CTX4000, PhotoAnglo, or other radar systems.

"IrateMonk":

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.



(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

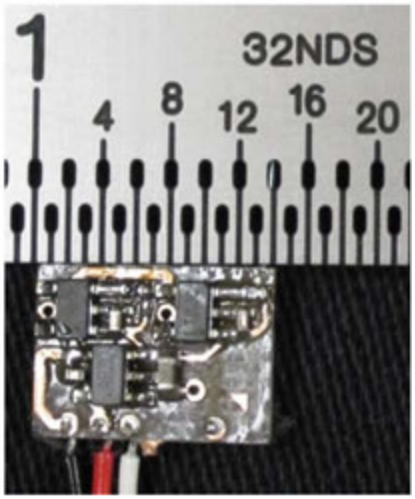
Unit Cost: $0

"SurlySpawn":

(TS//SI//REL TO USA,FVEY) Data RF retro-reflector. Provides return modulated with target data (keyboard, low data rate digital device) when illuminated with radar.

(U) Capabilities

(TS//SI//REL TO USA,FVEY) SURLYSPAWN has the capability to gather keystrokes without requiring any software running on the targeted system. It also only requires that the targeted system be touched once. The retro-reflector is compatible with both USB and PS/2 keyboards. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities will include laptop keyboards.

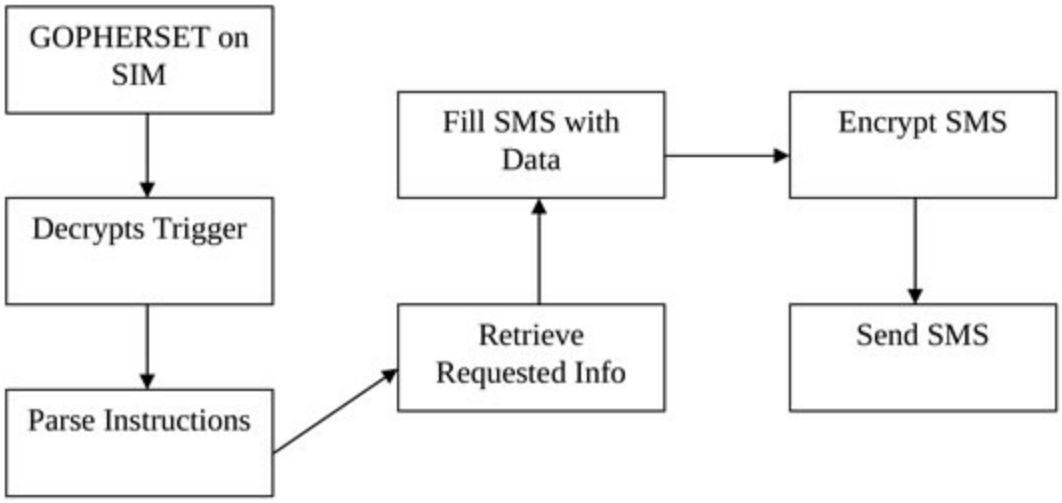


(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The board taps into the data line from the keyboard to the processor. The board generates a square wave oscillating at a preset frequency. The data-line signal is used to shift the square wave frequency higher or lower, depending on the level of the data-line signal. The square wave, in essence, becomes frequency shift keyed (FSK). When the unit is illuminated by a CW signal from a nearby radar, the illuminating signal is amplitude-modulated (AM) with this square wave. The signal is re-radiated, where it is received by the radar, demodulated, and the demodulated signal is processed to recover the keystrokes. SURLYSPAWN is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

"GopherSet":

(TS//SI//REL) GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls Phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

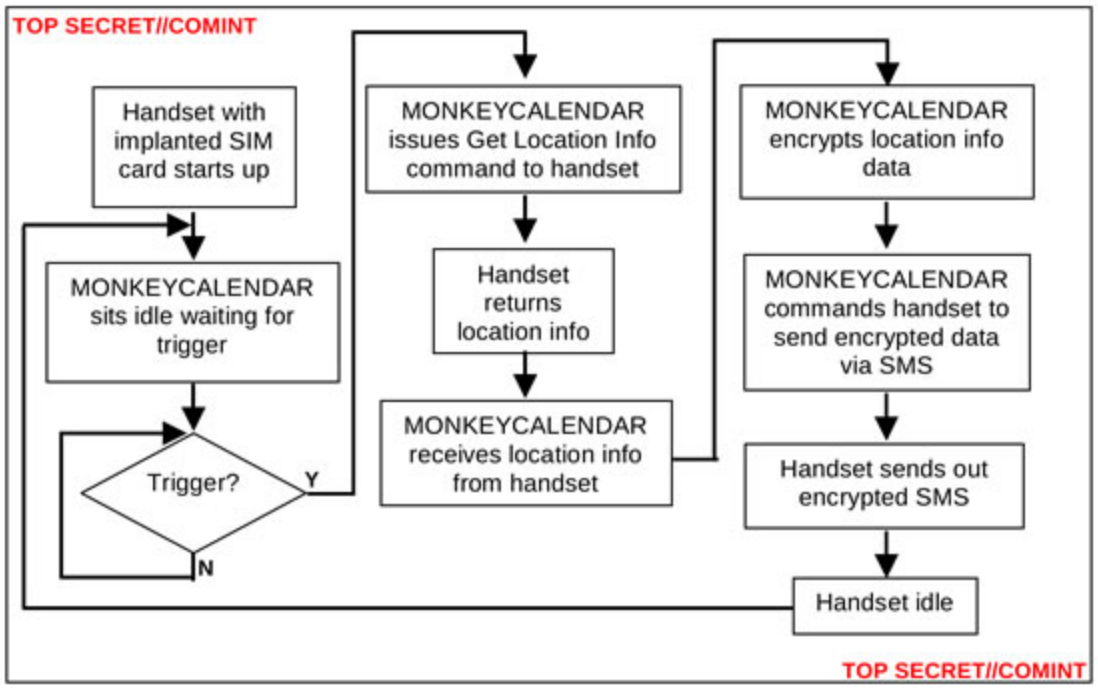


(U//FOUO) GOPHERSET – Operational Schematic

(TS//SI//REL) Modern SIM cards (Phase 2+) have an application program interface known as the SIM Toolkit (STK). The STK has a suite of proactive commands that allow the SIM card to issue commands and make requests to the handset. GOPHERSET uses STK commands to retrieve the requested information and to exfiltrate data via SMS. After the GOPHERSET file is compiled, the program is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning. In both cases, keys to the card may be required to install the application depending on the service provider's security configuration.

"MonkeyCalendar":

(TS//SI//REL) MONKEYCALENDAR is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls geolocation information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).



(U//FOUO) MONKEYCALENDAR – Operational Schematic

(TS//SI//REL) Modern SIM cards (Phase 2+) have an application program interface known as the SIM Toolkit (STK). The STK has a suite of proactive commands that allow the SIM card to issue commands and make requests to the handset. MONKEYCALENDAR uses STK commands to retrieve location information and to exfiltrate data via SMS. After the MONKEYCALENDAR file is compiled, the program is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning. In both cases, keys to the card may be required to install the application depending on the service provider's security configuration

"Genesis":

(S//SI//REL) Commercial GSM handset that has been modified to include a Software Defined Radio (SDR) and additional system memory. The internal SDR allows a witting user to covertly perform network surveys, record RF spectrum, or perform handset location in hostile environments.

(S//SI//REL) GENESIS Handset

(S//SI//REL) The GENESIS systems are designed to support covert operations in hostile environments. A witting user would be able to survey the local environment with the spectrum analyzer tool, select spectrum of interest to record, and download the spectrum information via the integrated Ethernet to a laptop controller. The GENESIS system could also be used, in conjunction with an active interrogator, as the finishing tool when performing Find/Fix/Finish operations in unconventional environments.

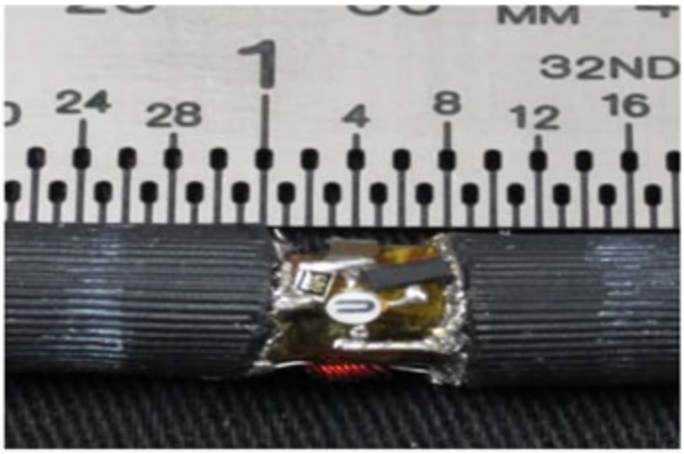
- **(S//SI//REL) Features:**
  - Concealed SDR with Handset Menu Interface
  - Spectrum Analyzer Capability
  - Find/Fix/Finish Capability
  - Integrated Ethernet
  - External Antenna Port
  - Internal 16 GB of storage
  - Multiple Integrated Antennas
- **(S//SI//REL) Future Enhancements:**
  - 3G Handset Host Platform
  - Additional Host Platforms
  - Increased Memory Capacity
  - Additional Find/Fix/Finish Capabilities
  - Active Interrogation Capabilities

“RageMaster”:

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.



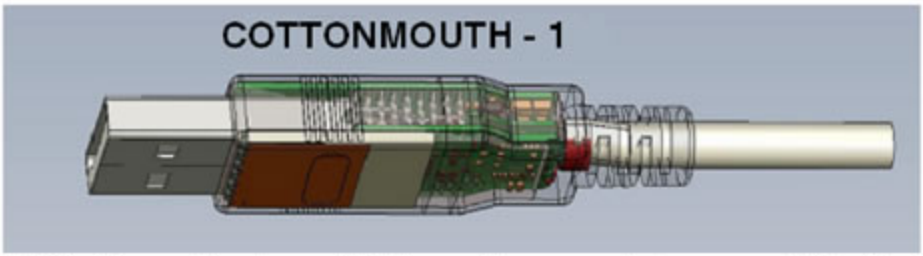
(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

Unit Cost: $ 30

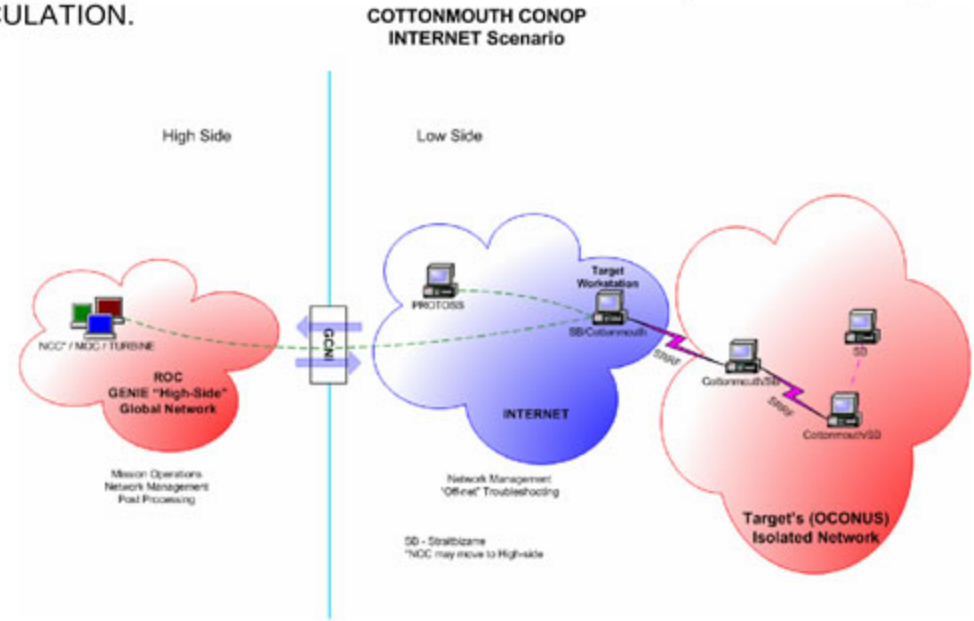
"CottonMouth":

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.



(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.



Status: Availability – January 2009

Unit Cost: 50 units: $1,015K