;
;
; 06/04/13 10:39 AM
;
;;;;neotech b1

>> GOOD MORNING.
IT'S MY PLEASURE TO WELCOME YOU
TO OUR MOBILE SECURITY FORUM.
I'M DELIGHTED YOU'RE ALL HEAR TO
LEARN WITH US AND TEACH US AS
WELL.
SINCE THIS IS A POST-SEQUESTERED
ERA GOVERNMENT EVENT.
THERE'S NO COFFEE OR WATER AND I
WANT TO WARN YOU IN ADVANCE
YOU'LL HAVE ACCESS TO BATHROOMS
AND THERE'S A WATER FOUNTAIN IF
YOU BROUGHT YOUR OWN BOTTLE.
SO THOSE WHO DID NOT COME
PREPARED WILL HAVE TIME FOR
PROVISIONS.
A FEW NOTES WITH THE Q AND A
WE'LL NOT HAVE SPECIFIC Q AND A
PORTIONS FOR PANELS SO IF YOU
HAVE A QUESTION YOU CAN RIGHT IT
DOWN ON THE Q AND A CARD,
THERE'S SOME ON THE TABLE WITH
THE MATERIALS.
HOLD IT UP IN THE AIR, SOMEONE
WILL COME AND GET IT AND DELIVER
IT TO THE MODERATOR AND WE'LL
TRY TO GET THROUGH AS MANY OF
THOSE QUESTIONS AS WE CAN BUT
WE'LL BE TAKEN ONLY WRITTEN
QUESTIONS.
WE'LL ALSO, BECAUSE WE'RE VERY
HIGH TECH AT THE FTC TAKING
QUESTIONS OVER OUR FACEBOOK PAGE
IN THE WORKSHOP STATUS THREAD
AND VIA E-MAIL TO OPA FOR OFFICE
OF PUBLIC AFFAIRS AT FTC.GOV AND
THE STAFF WILL BE LIVE-TWEETING
FROM THE FTC TWITTER ACCOUNT
USING THE HASHTAG FTC MOBILE.
SPEAK OF MOBILE, TAKE THIS

OPPORTUNITY TO TURN OFF YOUR
MOBILE DEVICE AND LET ME QUICKLY
RUN THROUGH OUR SECURITY
PROCEDURES.
ANYONE WHO LEAVES THE BUILDING
WITHOUT THE FTC BADGE WILL BE
REQUIRED TO GO BACK THROUGH
SECURITY INCLUDING THE METAL
DETECTERS SO PLEASE TIME YOUR
RETURN ACCORDINGLY.
IF THE EVENT OF A FIRE OR
EVACUATION LEAVE IN AN ORDERLY
BUILDING AND LOOK ACROSS TO OUR
CENTER IN THE RALLYING POINT TO
THE RIGHT SIDE OF THE BUILDING
IS WHERE YOU'LL MEET AND
THERE'LL BE A PERSON ACCOUNTING
FOR THE ATTENDEES IN THE EVENT
IT'S SAFER TO REMAIN INSIDE
YOU'LL BE TOLD WHERE TO GO.
IF YOU SPOT SUSPICIOUS ACTIVITY
PLEASE REPORT AND BY
PARTICIPATING YOU'RE AGREEING
ANYTHING YOU SUBMIT WILL BE ON
ONE OF THE SOCIAL MEDIA SITES.
I'D LIKE TO INTRODUCE EDITH
RAMIREZ FOR OPENING REMARKS TO
SET THE STAGE FOR THE REST OF
THE DAY.
THANK YOU TO THE CHAIRWOMAN AND
FOR ALL YOU FOR PARTICIPATING.
>> THANK YOU, EMILY AND THANKS
TO ALL OF YOU FOR BEING HERE
TODAY AND WELCOME TO THE FTC'S
MOBILE SECURITY FORUM.
IT'S NO EXAGGERATION TO SAY
WE'RE IN THE MIDST OF A MOBILE
REVOLUTION.
TODAY CONSUMERS BUY TWICE AS
MANY MOBILE DEVICES AS THEY DO
PCs.
NEARLY A THIRD OF CONSUMERS WHO
USE THEIR PHONES TO GET TO THE
INTERNET SAY IT'S THE PRIMARY
WAY OF REACHING THE WEB AND
STARTING TO SEE THE RISE OF THE

MOBILE-ONLY USER.
SMARTPHONES ACCOUNTED FOR MOST OF THE USAGE.
SMARTPHONE USERS REACH FOR THEIR PHONES AN ASTONISHING 150 TIMES A DAY TO SEND A TEXT, CHECK FOR E-MAIL, OCCASIONALLY MAKE A PHONE CALL, SURF THE WEB OR USE AN APP.
TODAY THOUGH WE'LL BE TURNING AWAY FROM OUR ADDICTIVE SMARTPHONES AND TABLETS OR SO I HOPE TO CONSIDER THE CURRENT STATE OF MOBILE SECURITY.
EMERGING THREATS AND THE MEASURES INDUSTRY, GOVERNMENT AND CONSUMERS CAN TAKE TO PROTECT AGAINST SECURITY RISKS.
OUR INTEREST IN MOBILE SECURITY IS AN OUTGROWTH OF THE FTCs BROAD MANDATE TO PROTECT CONSUMERS INCLUDING PROTECTING THEM TO THE THREATS AND ENJOYMENTS OF THE NEW TECHNOLOGIES.
IN THE LAST DECADE, THE FTCs BEEN AT THE FOREFRONT ALONG WITH OUR PARTNERS AT THE JUSTICE DEPARTMENT AND IN THE STATES OF THE FIGHT AGAINST SPYWARE ON THE DESK TOP CON COMPUTER AND BROAD ACTIONS AGAINST ROGUE IPSPs WHO DISTRIBUTE MALWARE TO NUISANCE ADDWARE THAT DELIVER POP-UP ADS.
WE BROUGHT A NUMBER OF CASES INCLUDING A SWEEP AGAINST MARKETERS OF SCAREWARE EXAMS THAT OPERATED IN THE U.S. AND ACROSS THE GLOBE.
AS CONSUMERS MIGRATE TO SMARTPHONES AND TABLETS IN RECORD NUMBERS WE'RE NOW TURNING OUR ATTENTION TO THE SECURITY OF THE MOBILE ENVIRONMENT.
WE HAVE THREE MAIN TOOLS AT OUR DISPOSAL.

LAW ENFORCEMENT, CONSUMER AND BUSINESS EDUCATION AND POLICY.
IT INCLUDES DIALOG AND ADVOCATING BEST PRACTICES.
ON THE ENFORCEMENT FRONT WE'VE ADDRESSED MOBILE SECURITY WITH THE FIRST CASE IN THIS ARENA.
IN FEBRUARY THE COMMISSION ALLEGED THAT HTC AMERICA THE MOBILE DEVICE MAKER INTRODUCED AN ARRAY OF SECURITY VULNERABILITIES IN THE COURSE OF CUSTOMIZING ITS MOBILE DEVICES THEREBY PUTTING RISKS AND CHARGED THEM WITH DECEPTIVE AND UNFAIR PRACTICES TO RESOLVE THE PRACTICES HTC WILL UNDER GO IN INDEPENDENT SECURITY AUDITS FOR 20 YEARS.
THE SETTLEMENT HAS A PROVISION FOR THE FIRST OF ITS KIND IN ANY OTHER U.S. OR FOREIGN AGENCY ORDER, A THAT HTC DEVELOP AND RELEASE SOFTWARE PATCHES TO FIX THE VULNERABILITIES ON MILLIONS OF ITS DEVICES.
THE CASES LIKE HTC DEMANDS SOPHISTICATED TOOLS AND TO MAKE THEM POSSIBLE WE CREATED A FORENSIC MOBILE LAB TO CONDUCT RESEARCH AND INVESTIGATIONS.
WE'VE BROUGHT IN DISTINGUISHED TECHNOLOGISTS LIKE STEVE BELLANIN AND ED FELTON OF PRINCETON AND CREATED AMOBILE UNIT TO ENSURE WE'RE ALERT TO MOBILE ISSUES IN ALL OF OUR CONSUMER-PROTECTION WORK.
AS OF THE FTC'S SECOND TOOL, EDUCATION THE GOOD NEWS IS SOME OF YOU WITH US TODAY ALREADY OFFER AN ARRAY OF INNOVATIVE TECHNOLOGIES SOME OF WHICH ARE FREE TO HELP USERS SECURE THEIR MOBILE DEVICES BUT MORE WORK NEEDS TO BE DONE.

FOR OUR PART, EARLIER THIS YEAR
THE FTC RELEASED AN ONLINE
BUSINESS GUIDE TO ENCOURAGE
ABOUT SECURITY AND OFFERS
PRACTICAL TIPS AND GUIDANCE ON
HOW TO DO THAT.
FOR CONSUMERS WE OFFER EXTENSIVE
MATERIALS TO HELP THEM STAY SAFE
AND SECURE WHETHER ON THEIR HOME
COMPUTE OR DEVICE WE HAVE TIPS
ON MOBILE MALWARE AND UPDATES
FOR MOBILE OPERATING SYSTEMS.
AND WITH TODAY'S FORUM, THE FTC
IS CONTINUING IT'S POLICY WORK
IN THE MOBILE SPHERE.
IN THE PAST YEAR WE'VE HOSTED
ROUNDTABLES EXPLORING MOBILE
CRAMMING, MOBILE PAYMENTS AND
PRIVACY AND ADVERTISING
DISCLOSURES.
THIS SERIES OF POLICY DIALOGS
REFLECTS THE HIGH PRIORITY WE
PLACE ON ENSURING THAT THE FTC
ITSELF, INDUSTRY, CONSUMER
GROUPS AND OTHER STAKEHOLDERS
ARE ALL FULLY ATUNED TO THE
CONSUMER PROTECTION ISSUES
PRESENTED BY THE EXPLOSIVE
GROWTH OF MOBILE TECHNOLOGY.
AS PART OF TODAY'S PROGRAM WE
HAVE VOICES FROM ACADEMIA AND
CONSUMER ORGANIZATIONS TO ENGAGE
IN WHAT I'M CONFIDENT WILL BE A
RICH AND ROBUST DISCUSSION.
MOBILE DEVICES DEPEND ON MANY
DIFFERENT PLAYERS.
AMONG THEM DEVICE MANUFACTURES,
CHIP MAKERS, APP STORES, APP
DEVELOPERS AND EACH SERVES A
UNIQUE BUT CRITICAL FUNCTION IN
THE USER EXPERIENCE.
SO I'M ESPECIALLY PLEASED TO
HAVE SUCH EXCELLENT
REPRESENTATION ACROSS THE
ECO-MOBILE SYSTEM.
I APPRECIATE YOUR WILLINGNESS TO

SHARE YOUR EXPERTISE AND WELCOME
YOUR THOUGHTS ON HOW TO
COLLABORATE TO ENSURE MOBILE
TECHNOLOGY IS SAFE.
GIVEN THE EXPONENTIAL GROWTH OF
MOBILE THERE'S NO ROOM FOR
COMPLACENCY TO KEEP IT SAFE AND
SECURE AND I'M HOPING WE'LL

INSPIRE ACTION AND INNOVATION
WE'LL BEGIN WITH AN OVERVIEW OF
THE MOBILE ECO SYSTEM.
STEVE DONOVAN.
HE'S A RENOWNED EXPERT ON
NETWORK SECURITY AND FORTUNATE
TO HAVE HIM WITH US THIS YEAR
AND THIS MORNING TO LAY THE
GROUNDWORK FOR TODAY'S PROGRAM.
BEFORE I HAND THE PROGRAM OVER
TO STEVE I WANTED TO TAKE THE
OPPORTUNITY TO THANK YOU ALL
AGAIN FOR BEING WITH US THIS
MORNING AND ALSO WANT TO TAKE
THIS OPPORTUNITY TO THANK THE
FTC TEAM WHO PUT THIS EVENT
TOGETHER.
INCLUDING EMILY BURTON, DAN
SALBERG AND PAUL NOME.
NOW JOIN ME IN WELCOMING STEVE
BELLOVIN.
>> THANK YOU, CHAIRWOMAN
RAMIREZ.
I APOLOGIZE FOR HAVING SLIDES.
MY YEARS AT AT&T LABS RENDER ME
WITHOUT BEING ABLE TO SPEAK
WITHOUT SLIDES.
WE'LL BE TALKING ABOUT THE
MOBILE SPACES.
WHAT ARE ALL THE DIFFERENT
PIECES.
IT'S NOT JUST ONE PROBLEM.
THERE'S A SAYING THAT THE
ATTACKER CAN ATTACK ANYWHERE THE
DEFENDER HAS TO DEFEND

EVERYWHERE WHICH MEANS YOU HAVE
TO KNOW WHERE EVERYWHERE IS.
IT'S NOT JUST ONE LAYER.
THERE'S THE OLD STORY ABOUT THIS
19th CENTURY PHYSICIST IN HOW
THE UNIVERSE AND THE WOMAN CAME
TO SAY YOU FORGOT MY FAVORITE
THEORY ABOUT THE UNIVERSE RIDING
ON THE BACK OF A TURTLE AND SHE
SAYS IT RIDES ON A BIGGER
TURTLE.
MOBILE DEVICES CAN HAVE SECURITY
FLAWS IN ANY LAYER AND SECURITY
FEATURES FROM THE CLIPS TO THE
APPLICATIONS.
THEY COME FROM MANY PIECES FROM
MANY PLACES.
WE AS DEFENDERS NEED TO PROTECT
THEM ALL.
WE CAN START WITH THE CHIPS.
THE BASIC CHIP THAT'S IN MOST
PHONES THESE DAYS THE GSM AND LD
FIRMS THE SIM CHIP.
THIS TENDED TO BE A SECURE CHIP
THAT SAYS WHO YOU ARE, YOUR
PHONE NUMBER AND SO ON.
YOU CAN READ THIS OUT AND
IMPERSONATE YOU PERHAPS.
SOME OF THE NEWER PHONES HAVE
THE NEW CHIPS USED IN WALLETS
LOVELY FEATURE BUT YOU CAN PAY
FOR SOMETHING BUT IT'S IF IT'S
NOT PROPERLY DESIGN OR SECURE
SOMEONE CAN READ OUT YOUR BANK
ACCOUNT NUMBER OR BY ACCIDENT.
YOU PUT YOUR WALLET ON THE
COUNTER NEXT TO YOU WHILE YOU
TAKE OUT A CREDIT CARD TO PAY
AND THE MERCHANT'S NFC READER IS
READING YOUR PHONE, PERHAPS
INSTEAD OF YOUR CREDIT CARD YOU
INTENDED TO PAY WITH.
YOU PAY WITH CASH AND YOU PAY
WITH YOUR NFC CHIP,
SIMULTANEOUSLY.
ISN'T THAT A GREAT STUNT.

THERE ARE MANY WIRELESS
INTERFACES BY WHICH ATTACKS CAN
ENTER THE PHONE.
THE BLUETOOTH THAT SEEM TO BE
TALK TO THEMSELVES ARE NOT
STRANGE.
THE MOBILE HOT SPOTS.
I SEE WHAT LOOKS LIKE A WI-FI
HOT SPOT OVER THERE AND GPS.
THEY'RE SECURITY MECHANISM THAT
DEPEND ON YOUR LOCATION, IF
SOMEONE CAN SPOOF YOUR LOCATION,
BAD THINGS CAN HAPPEN.
AND OF COURSE THE OVER THE AIR
WIRELESS INTERFACE WITH NETWORKS
AND CDMA OR LDE OR WHAT OTHER
VARIETY WE SEE IN THE COMING
YEARS THESE ARE ALL BAD THINGS
THAT CAN HAPPEN NOT PROTECTED.
THERE ARE HALF A DOZEN IMPORTANT
ONES TODAY OR COMING IN THE NEAR
FUTURE.
IOS FOR APPLE ON iPHONES AND
TABLETS AND THE ANDROID PHONES
FROM MANY DIFFERENT
MANUFACTURES, WINDOWS PHONE,
ESPECIALLY WINDOWS PHONE 8, THE
NEWLY REVISED BLACKBERRY OS.
FORTHCOMING COMES WITH OS
PROBABLY MORE COMING.
UNCLEAR HOW MANY THE MARKET WILL
SUPPORT BUT WE HAVE LEARNED IN
THE PC WORLD THAT IT DOESN'T
TAKE THAT MANY INSTANCES OF A
DEVICE TO SUPPORT A VIABLE
ECOSYSTEM FOR MALWARE AND THEY
CAN SPREAD THROUGH LOW DENSITIES
OF PHONES.
WE HAVE DIFFERENT HARDWARE
PLATFORMS AND iPHONES AND
BLACKBERRIES WHICH BELONG TO ONE
MANUFACTURE BUT THEY'RE
MANUFACTURED VERY OFTEN
ESPECIALLY THE iPHONE BY
CONTRACT MANUFACTURES.
THERE'S BEEN SECURITY PROBLEMS

IN THE PAST COMING FROM THE FACTORY.
I'VE SEEN NEWS REPORTS OF DIGITAL PICTURE FRAMES COMING WITH VIRUSES ON THEM WHEN YOU PLUG THEM INTO YOUR COMPUTER IT SPREAD THE VIRUS THROUGH THE COMPUTER.
ACCIDENTAL NO DOUBT, BUT IT'S A CONCERN.
MANY OTHER MANUFACTURES OF HARDWARE ESPECIALLY ANDROID PHONES AND DIFFERENT COMPANIES MANUFACTURE DIFFERENT VARIETIES OF ANDROID PHONES AND THE iPHONES IT'S HARD TO TELL HOW THEY'LL DEVELOP BUT THERE ARE DIFFERENT MANUFACTURES.
A NUMBER OF PROBLEMS START BECAUSE THE USER IS CONFUSED BY AN INADEQUATE DESIGN.
THEY'RE NOT UNDERSTANDING WHAT THEY AGREE TO OR TAPPING TO.
WE HAVE DIFFERENT INTERFACES.
WE START WITH THE ONES THAT COME FROM THE OS VENDOR, APPLE, GOOGLE, MICROSOFT OR WHOEVER.
BUT DIFFERENT MANUFACTURE EASE SPECIALLY IN THE ANDROID WORLD ADD THEIR OWN CHANGES, ENHANCEMENTS, WHAT HAVE YOU TO THEM.
THIS IS THEIR PRODUCT DIFFERENTIATION.
THE PROBLEMS CAME FROM CHANGES AND THEY THOUGHT THERE WERE IMPROVEMENTS TO THE ANDROID PHONES TO ADD NEW FEATURES.
CARRIERS HAVE THEIR NEW FEATURES.
THAT'S PART OF THEIR DIFFERENTIATION AND THERE'S A VARIETY OF CALL IT, SKINS, TO STILL CHANGE IT.
THE AMAZON KINDLE AND BARNE'S AND NOBLE NOOK ARE ANDROIDS

UNDERNEATH WITH A NEW SKIN ON
THE ANDROID.
ALL THESE CHANGE THE USER
INTERFACE IN A WAY THAT MAY BE
BETTER OR NOT BUT IT'S
DIFFERENT.
APPS.
THERE ARE SO MANY MILLIONS, TEN
OF MILLIONS OF APPS.
ABOUT THAT MANY DIFFERENT
VENDORS.
SOME ARE VERY SMALL.
SOME ARE VERY LARGE.
THE LARGE ONES, IF THEY GET IT
WRONG IT'S A GOOD OPPORTUNITY
FOR THE MALWARE WRITERS.
THE SMALL ONES MAY NOT HAVE THE
SOPHISTICATION TO DO IT RIGHT.
SOME USE THIRD-PARTY LIBRARIES
AND SOME ARE NOT UPDATED WELL
AND HAVE WELL-KNOWN HOLES AND
MANY OF THE JAILBREAKS ARE DUE
TO THE APPS.
THEY'RE OFTEN INTERACTING WITH
REMOTE SERVERS IF THEY'RE NOT
ADEQUATELY SECURED AND A LOT
AREN'T RESEARCH HAS SHOWN.
WE HAVE SHOWN THAT THAT WAY AND
APP STORES RUN BY APPLE,
MICROSOFT, AMAZON AND GOOGLE AND
SMALLER APPS IN THE ANDROID
WORLD AND THEY'RE ALL THE
CONTENT SERVERS.
THERE'S BEEN VULNERABILITIES IN
THE PC WORLD WITH JUST VIEWING A
PICTURE WITH SOPHISTICATION TO
PENETRATE THE MACHINE AND
THERE'S A LOT OF INFORMATION AT
RISK.
WHO YOU ARE, WHAT ARE YOU DOING.
I WON'T SAY THE -- THE KEY TAPS
AS YOU LOG INTO SOMETHING.
WHERE YOU ARE.
LOCATION TRACKING BY PEOPLE WHO
WANT TO STALK YOU.
WHAT ELSE YOU HAVE DONE?

THE HISTORY THAT'S KEPT BY A LOT
OF THESE APPS.
YOUR CONTACT LIST.
WHO YOU TALK TO, YOUR CALENDAR,
WHERE YOU ARE AND SO MUCH MORE.
ALL OF THIS IS AT RISK TO A
MALICIOUS APP, PENETRATED
OPERATING SYSTEM IF THERE AREN'T
SUFFICIENT PROTECTIONS AT EVERY
LAYER.
IN THE PC WORLD THE LAPTOP
WORLD, WE'VE GOTTEN USED TO
PATCHES.
WE HAVE AN OPERATING SYSTEM.
THE VENDOR SUPPLIES PATCHES.
WE HAVE AN APPLICATION, THE
APPLICATION VENDOR SUPPLIES
PATCHES.
IT'S MORE COMPLICATED IN THE
MOBILE DEVICE WORLD.
WE HAVE MANY DIFFERENT VENDORS
BUT THEY DON'T CONTROL THE
PATCHES FOR THE MOST PART.
THEY DON'T CONTROL IT BY
THEMSELVES BECAUSE THEY SELL THE
PHONES VIA THE CARRIERS.
APPLE CAN DO THE PATCHES ITSELF
DIRECTLY BUT IF A RANDOM -- IF A
FLAW IS FOUND SAY IN ANDROID
GOOGLE WILL FIX IT BUT THEN IT
HAS TO GO TO THE MANUFACTURE OF
THE PHONE BECAUSE IT MAY
INTERACT AND TO THE CARRIER AND
THEY ULTIMATELY SHIP TO THE
USER.
THE APPLICATIONS ARE DISTRIBUTED
THROUGH APP STORES IT HAS TO GO
THROUGH THE APP STORE APPROVAL
PROCESS FOR IOS TO GET OUT THERE
AND THEY'RE BUILT ON THIRD-PARTY
LIBRARIES AND THEY'RE NOT ALWAYS
TRACKING THE CHANGES, UPDATES
AND FIXES TO THE THIRD-PARTY
LIBRARIES.
SO IT'S A COMPLEX AND LARGE MIX
OF PLAYERS WHO HAVE TO COOPERATE

AND ADD TO THAT THE SHORT LIFE
SPAN OF THE PHONE.
18 MONTHS IS THE AVERAGE TIME
SOMEONE OWNS A PHONE AND WHAT WE
SEE IS MANUFACTURES SOMETIMES
DON'T WANT TO REPAIR THE PATCH
BECAUSE THEY KNOW THERE'S A NEW
RELEASE COMING OUT SOON YOU'RE
PROBABLY GOING TO BUY EXCEPT IF
YOU'RE ONE OF THE PEOPLE WHO
HOLDS ON TO THE PHONE FOR TWO
AND A HALF COMPARED TO ONE AND A
HALF YOU MAY HAVE A LONG PERIOD
WHERE THE PHONE AND APPS ARE NOT
PATCHED.
IT'S A VERY COMPLEX PROCESS AND
THE PATCH MECHANISM HAS BEEN
WORKING DECENTLY IN THE LAPTOP
AND PC AND MAC WORLD.
DOZENS WORK AS WELL IN THE
MOBILE DEVICE WORLD.
GIVEN THE BUSINESS
RELATIONSHIPS, THIS IS A
TECHNICAL PROBLEM.
IT'S HARD TO SHIP ONE PATCH FROM
SAY GOOGLE OUT DIRECTLY TO THE
USER WITHOUT TESTING BY THE
MANUFACTURER AND CARRIER AND BY
TO THE APP VENDOR.
IT IS NOT AN EASY PROBLEM.
SO IT IS TURTLES ALL THE WAY
DOWN.
WE AS THE DEFENDERS HAVE TO FIX
EVERY LAYER DESPITE THE
COMPLEXITY OF THE BUSINESS
RELATIONSHIPS, THE WHOLE
ECOSYSTEM.
THANK YOU.

>> I AM EMILY BURTON.
LET HE START THE PANELS.
TO MY LEFT IS OMAR KHAN THE
CO-CEO OF A MOBILE SECURITY
COMPANY THAT PROVIDES MOBILE
APPS TO PROTECT FROM MALWARE
THEFT AND LOSS AND TO HIS LEFT

IS GARETH McLACHLAN OF ADAPTIVE MOBILE.
ANOTHER SECURITY COMPANY THAT FIXES NETWORK OPERATORS AND THEIR SUBSCRIBERS AND TO HIS LEFT IS DAN GUIDO FROM AN INFORMATION COMPANY TO ENABLE COMPANIES TO MAKE BETTER DEFENSE DECISIONS AND TO HIS LEFT IS PATRICK TRAYNOR FROM GEORGIA TECH ON MOBILE SYSTEM AND THE RISKS OF MOBILE MALWARE.
A PRINTED BIO-SHEET IS AVAILABLE IN YOUR FOLDER SO REFER TO THAT FOR THE DETAILS ON THE PANELISTS AND OTHERS.
TO KICK OFF THE PANEL, OMAR WILL SUMMARIZE THE RESEARCH ON MOBILE MALWARE.
WE'LL TURN IT OVER TO YOU.
>> THANKS.
>> GREAT.
THANKS FOR HAVING ME.
STEVEN DID A GREAT JOB OF SETTING THE LANDSCAPE FOR WHAT'S HAPPENING IN THE MOBILE INDUSTRY I SPENT THE LAST 13-PLUS YEARS ON THE MANUFACTURERING SIDE AS WELL AS OEM-CARRIER APPLICATIONS SIDE OF THE MOBILE INDUSTRY.
IT'S SAFE TO SAY WHAT WE'RE ALL MOST EXCITED ABOUT IN TERMS OF THE INNOVATION WITHIN MOBILE DEVICES AND APPLICATIONS FROM AN OPERATING SYSTEM PERSPECTIVE IS THE VULNERABILITIES.
WE APPROACH IT AT NQ MOBILE FROM ENABLING CONSUMERS TO BE EMPOWERS OR ENTERPRISES TO BE EMPOWERED TO PROTECT THEMSELVES ON THE DEVICES TO TRUST THE THINGS THEY WANT TO DO USING THE

DEVICES.
GOING FORWARD IT'S NOT FEAR WE WANT TO BE CONSUMERS LEFT WITH

IT'S EMPOWERMENT OF THEIR DATA, DEVICES AND WHAT THOSE DEVICES ARE CAPABLE OF.
AS WE HEAD FORWARD AND FAST FORWARD TO THE NEXT THREE TO FIVE TO TEN YEARS OF WHAT THE DEVICES ARE CAPABLE OF THEY'RE

POWERFUL AND AS THE DEVICES BECOME CONDUITS FOR OTHER DEVICES WHETHER THEY'RE PERSONAL HEALTH CARE OR MOBILE-PAYMENT ECOSYSTEMS THEY'LL BE CONDUITS FOR PERSONAL INFORMATION AND THE CONTEXT THAT MAKES THOSE DEVICES RICH IN TERMS OF THE INFORMATION THEY HAVE AND CAN PROVIDE.
THERE'S A YOUTUBE VIDEO SOMEONE TOLD ME ABOUT THAT TALKED ABOUT MOBILE PAYMENTS AND I THINK IT WAS AT AN IN AND OUT IN CALIFORNIA AND COMPARED PAYING WITH YOUR PHONE TO THE CREDIT CARD.
THE CREDIT CARD I THINK MOST WOULD AGREE IS A KILLER APP.
THE ABILITY TO SWIPE IN LESS THAN TEN SECONDS AND PUT IT IN YOUR WALLET IS FAIRLY QUICK.
SO MOBILE DEVICES JUST FROM THE PERSPECTIVE OF IT REPLACING A CREDIT CARD IS NOT REALLY WHAT'S GOING TO DRIVE ADOPTION OF MOBILE PAYMENTS, IT'S THE FACT THAT IT HAS CONTEXT AND PROVIDES INFORMATION TO PAYMENT VENDORS TO MERCHANTS THAT MAKES THE TRANSITION MUCH MORE RICH FOR A CONSUMER.
THAT'S REALLY I THINK WHAT'S GOING TO DRIVE THAT ADOPTION BUT IT'S ALSO THOSE ENVIRONMENTS THAT CREATE ENVIRONMENTS FOR HACKERS AND MALICIOUS HACKERS TO EXPLOIT CONSUMERS.
I'M GOING QUICKLY -- I DON'T

NEED TO NECESSARILY GO THROUGH EACH SLIDE BUT WE'RE A MOBILE SECURITY COMPANY FOCUSSED ON END POINT AND PROVIDE SOLUTIONS FOR CONSUMERS, ENTERPRISES, CARRIERS AND FROM THE ANTI-VIRUS AND ENCRYPTION STANDPOINT AND HELP TO NOT LOSE DATA AND WHEN YOU DOWNLOAD THIRD-PARTY APPLICATIONS BEING ABLE TO PERSONALLY ENCRYPT YOUR OWN DATA FROM A CONTEXT AND COMMUNICATIONS PERSPECTIVE IS WHAT WE PROVIDE AND PROVIDE A SET OF SOLUTIONS FOR PARENTS TO PROTECT THEIR KIDS ON THEIR SMARTPHONES IN TERMS OF PARENTAL CONTROL AND LOCATION AND MANAGE APPLICATIONS AND PERSONAL CONTENT AND HELP TEACH RESPONSIBLE BEHAVIOR TO KIDS ABOUT USING MOBILE DEVICES AND WE CAN TALK MORE ABOUT THAT ON THE PANEL.
FROM THE PERSPECTIVE OF HACKERS, MALWARE IS VERY MUCH ON THE RISE.
WE'VE SEEN A HUGE INCREASE OVER THE LAST THREE YEARS ALONE IN THE PIECES OF MALWARE DISCOVERED BY OURSELVES AND COLLEAGUES IN THE INDUSTRY.
LAST YEAR WE DISCOVERED 65,000 UNIQUE PIECES OF MALWARE IDENTIFYING NEARLY 33 MILLION INFECTED DEVICES AND I GET THE QUESTION A LOT, ARE WE HERE IN THE U.S. IMMUNE TO MALWARE ATTACKS OR HACKS ON OUR DEVICES.
WE'RE NOT.
THERE IS NO CONCEPT OF A DIGITAL BORDER OUT THERE.
SO ATTACKS THAT EMANATE FROM VARIOUS COUNTRIES OR ENVIRONMENTS AROUND THE WORLD REALLY CAN SPREAD QUICKLY

THROUGH MOBILE ENVIRONMENTS.
IN JUST THE FIRST QUARTER ALONE
WE DISCOVERED 25,000 NEW PIECES
OF MALWARE.
IT'S SOMETHING GROWING TODAY
BECAUSE OF THE POWER OF ANDROID.
IT'S NOT TO SAY THAT ANDROID IS
-- IT'S BE AN AMAZING OPERATING
SYSTEM LEADING TO THE INNOVATION
WE'RE SEEING BUT IT'S THE SAME
CAPABILITIES BEING EXPOSED TO
DEVELOP RICH APPLICATIONS THAT
MALWARE AND MALICIOUS HACKERS
ARE TARGETING.
I WENT THROUGH THIS.
IF WE THINK OF SOME OF WHERE THE
INFECTIONS RUN MOST RAMPANT,
CHINA, INDIA, RUSSIA, U.S. ,
THAILAND, SAUDI ARABIA THEY'RE
HIGHEST ON THE INFECTION LIST.
IF YOU REWIND THE CLOCK FOUR
YEARS AND ASK YOURSELVES WHY
THIGH STARTED TO HAPPEN AS OIS
AND ANDROID STARTED TAKING OFF
APP STORES AND REGULATED APP
STORES FOCUSSED ON WESTERN
MARKETS LIKE THE U.S. OR WESTERN
EUROPE.
IT LEFT A LOT OF MARKETS SUCH AS
CHINA, INDIA, RUSSIA AND OTHER
EMERGING MARKETS TO HAVE A
LARGER ECOSYSTEM OF APP STORES
AS STEVEN MENTIONED.
WE PROBABLY STAN 5 MILLION
APPLICATIONS AND DISTRIBUTE
AROUND FOUR MILLION MARKET
PLACES.
THERE'S A SIGNIFICANT NUMBER OF
MARKET PLACES THEY CAN BE

PUBLISHED AND REPUBLISHED
WHETHER IT'S THROUGH LINKS OR
TEXT MESSAGES IT'S EASIER TO GET
THOSE AS WELL.
ACTUALLY, ONE THING WE'RE

TALKING ABOUT IS THERE'S A LOT
OF DIFFERENT THREAT VECTORS AS
WELL WHETHER IT'S EXPLOITS,
SPYWARE, TROJANS MEANT TO TAKE
CONTROL OF DEVICES AND MALWARE
IS DISCOVERED TO COLLECT PROFIT
GIVEN THE DATA ON THE MOBILE
DEVICE MORE THAN THE PC.
THE PC IT SITS ON YOUR KITCHEN
TABLE, IT SITS IN AN ENVIRONMENT
AND OVER HALF OF AMERICANS ADMIT
TO SLEEPING WITH THEIR MOBILE
DEVICES UNDER THEIR PILLOW OR
BEDSIDE.
WE DON'T DO THAT WITH A PC.
SO THE INTIMACY WE HAVE WITH THE
MOBILE DEVICES AND DEPENDENCY
CREATES IT AS WELL.
WE DISCOVERED A MALWARE IN
JANUARY CALLED BIG-SHOCKER FOR
REPACKAGING.
I KNOW ONE OF MY COLLEAGUES ON
THE PANEL WELL TALK WITH THE
PACKAGING AS WELL AND IT
INFECTED OVER 6 MILLION DEVICES.
IT WAS DEPLOYED THROUGH
OTHERWISE LEGITIMATE APPLICATION
AND TAKING CONTROL OF TEXT
MESSAGES AND HACKING THE TRAFFIC
ASSOCIATED SO THERE'S A
SIGNIFICANT AMOUNT OF PROFIT TO
BE MADE FOR HACKERS.
IF THERE WEREN'T THEY WOULDN'T
TARGET THE DEVICES TO BEGIN
WITH.
THE OTHER THING WE'RE SEEING FOR
THE FIRST TIME LAST YEAR IT WAS
CONFIRMED WEEKEND THE INDUSTRY
THERE WAS A CROSS-OVER ATTACK
BETWEEN PC AND MOBILE WHERE WE
SAW THE ABILITY FOR MALWARE FROM
A PC TO BE DISTRIBUTED TO A
MOBILE DEVICE VIA TECH.
AS YOUR CONNECTING YOUR DEVICE
WHETHER THAT'S ANDROID OR
ANOTHER DEVICE IT WAS INSTALLING

ITSELF USING THE USB PORT ONTO
THE DEVICES IN THE FILE SYSTEMS
AND THAT CAN EMANATE AND
CONTINUE TO PROPAGATE THROUGH A
SYSTEM IN THE SAME WAY ANY OTHER
MALWARE CAN.
SO WHAT'S A REAL RISK?
FROM A RISK PERSPECTIVE IT'S NOT
JUST APP REPACKAGING BUT WHAT
WE'RE SEEING FROM A CONSUMER
PERSPECTIVE IS PEOPLE ARE
INSTALLING APPLICATIONS FROM
THIRD-PARTY SYSTEMS IT'S NOT
JUST GOOGLE PLAY OR REGULATED
MARKET SYSTEMS.
WE'RE SEEING THE SOCIAL
RECOMMENDATIONS LIKE GOOGLE PLAY
ARE EFFECTIVE WE LOOK AT STAR
RATINGS AND DESPITE BEING TWO OR
THREE APPLICATIONS WE AS
CONSUMERS HAVE BEEN TRAINED WE
LOOK FOR THE ONE WITH TEN
MILLION DOWNLOADS OR FIVE-STAR
RATINGS.
THE SELF-REGULATING ENVIRONMENT
OF MARKET PLACE IS ACTUALLY
QUITE GOOD BUT DOESN'T PROTECT
YOU FROM SIDE-LOADING AND THE
LARGEST GROUP IS TWEENS AND MY
SON IS A TWEEN AND WE NEED TO AS
PARENTS AND ADULTS OUR
RESPONSIBILITY IS TO PROTECT OUR
KIDS IN THESE ENVIRONMENTS
BECAUSE THESE PHONES ARE ALWAYS
WITH THEM AND THEY'RE NOT
NECESSARILY ALWAYS TRAINED TO
KNOW WHAT THE BEST WAY TO USE
THEIR MOBILE DEVICES ARE SO
THERE'S A TREMENDOUS AMOUNT OF
RESPONSIBILITY ON PARENTS TO
SECURE THEIR MOBILE DEVICES AND
WE TALKED ABOUT FRAGMENTATION OF
SYSTEMS.
WHAT'S THE HARM TO CONSUMERS?
SOCIAL-ENGINEERING BASED ATTACKS
AND ONE THING WORTH SAYING IS

PHISHING ATTACKS ARE MORE
EFFECTIVE ON A MOBILE DEVICE
THAN THEY'VE EVER BEEN ON A PC
AND THE FACT IS URLs ARE
OBSCURED.
YOU DON'T HAVE A FOUR AND A HALF
INCH SCREEN SO THE MOST OFTEN
YOU HAVE URLs OBSCURE YOU DON'T
KNOW YOU'RE HEADING OFF INTO AN
ENVIRONMENT WHERE A PHISHING
ATTACK IS HAPPENING AND YOU'RE
MO MORE PRONE AND VULNERABLE.
WE SCAN OVER TWO BILLION URLs
AND FOUND FIVE MILLION MALICIOUS
URLs AND MOBILE BROWSER
REDIRECTS THEY'RE ALL
WELL-DOCUMENTED.
I THINK WE'LL DISCUSS THEM PONE
PANEL.
WHAT COULD HAPPEN IN THE FUTURE?
WE TALKED ABOUT APP REPACKAGING
AND OTHER ATTACKS INCLUDING
PHISHING BUT METAMORPHIC WE AS
ANTI-MALWARE MAKERS CAN HELP
WITH MOBILE THREATS INCLUDING
MALWARE BUT AS APPS UPDATE
THEMSELVES ON THE CLIENT'S SIDE
OR THROUGH SERVER-BASED UPDATES
THEY CHANGE VERY QUICKLY AND
WE'LL SEE -- WE HAVEN'T SEEN IT
YET BUT WE'LL BELIEVE WE'LL SEE
THESE TYPES OF APPS START TO
PROPAGATE IN THE INDUSTRY AND WE
HAVE TO BE PREPARED FOR THEM
FROM A TECHNOLOGY PERSPECTIVE.
BOTNETS ARE DOCUMENTED IN LEGACY
AND WE HAVEN'T SEEN THEM ON THE
MOBILE DEVICE JUST YET BUT WITH
THE CONTINUED DEPLOYMENT OF
IP-BASED NETWORKS WE EXPECT THIS
MOBILE DEVICE BOTNET AND I'M
SURE GAR ETH WILL GIVE US MORE
UPDATE AND REVERSE ENGINEERED
ATTACKS.
IT'S A COMPLETE BREAKDOWN OF
REPACKAGING BUT WE USE

TECHNIQUES SUCH AS COMPARES TO
IDENTIFY WHERE AN APP HAS BEEN
HACKED OR MALICIOUS PAYLOAD HAS
BEEN ADDED BECAUSE THERE'S
DIFFERENCE IN FILE SIZE BUT AS
YOU DO REVERSE ENGINEERING YOU
CAN MINIMIZE THAT AND THE MORE
LEGACY-ORIENTED OPPORTUNITIES
FOR YOU TO DISCOVER THAT MALWARE
MAY NOT NECESSARILY BE THERE IN
THE FUTURE SO IT'S INCUMBENT
UPON US TO INNOVATE OR ENGINES.
I THINK IT GIVES A GOOD
BACKGROUND OF WHAT HAPPENING IN
OUR INDUSTRY.
REPRESENTING NOT JUST MYSELF BUT
300 PLUS ENGINEERS AT NQ MOBILE
AND DRIVING TRUST IN THE MOBILE
ECO SYSTEM AND GOING TO GO AHEAD
AND JOIN THE PANEL AT THIS
POINT.
THANK YOU.
>> I THINK YOU'RE PRESENTATION
RAISES A LOT OF GREAT TOPICS BUT
I WANT TO START BY ASKING YOU TO
GIVE US A SENSE OF HOW NQ
DEMOBILE THREATS.
YOU MENTIONED IN APRIL YOU FOUND
MORE THAN 7,000 MOBILE THREATS
BUT WHEN YOU SAY THAT, WHAT ARE
YOU TALKING ABOUT SPECIFICALLY?
>> WHEN WE'RE TALKING ABOUT THAT
SPECIFICALLY WE'RE TALKING MORE
ABOUT UNIQUE MALWARE SIGNATURES.
WHERE WE'RE UPDATING ONE OF OUR
DATABASES AND MALWARE DATABASE
TO CATCH OR IDENTIFY AND RESOLVE
THE THREATS BUT IT DOES GO
BEYOND THAT.
WHILE WE SIT HERE TALKING
SPECIFICALLY ABOUT MALWARE
INFECTING OR TARGETING A DEVICE
THROUGH THE MECHANISMS I TALKED
ABOUT WHETHER THEIR THIRD-PARTY
APP STORES OR MALICIOUS-BASED
CODES IT GOES THROUGH

PHISHING-BASED ATTACKS WHICH IS NOT NECESSARILY CAPTURED WHEN I TALK ABOUT WHEN YOUR PHISHED FOR A ONE-TIME PASSWORD BECAUSE YOU'VE BEEN TAKEN INTO A URL YOU WERE UNSUSPECTING.
IT'S A LEGITIMATE THREAT AND THAT'S SOMETHING THAT CAN HAPPEN ON ANDROID AND ANY MOBILE DEVICE.
THE FACT WE MAY SIT HERE THINKING WE'RE IMMUNE IF WE'RE CARING A WINDOW-BASED DEVICE THE WEB-BASED ATTACKS OR BROWSER-BASED ATTACKS ARE JUST AS SIGNIFICANT AND ONE CAN CREATE JUST AS MUCH PAIN FOR THE CONSUMER AS A MALWARE OR APP-BASED ATTACK.
IT GOES BEYOND THAT BUT SPECIFICALLY WHEN WE TALK ABOUT THOSE KINDS OF QUANTIFIABLE STATISTICS IT'S MALWARE-PLUS.
>> GARETH, WHEN YOU'RE LOOKING AT A THREAT WHAT DO YOU DEFINE A MOBILE THREAT IS?
>> WE DON'T SELL TO CORPORATE SO WE'RE NOT INTERESTED TO GET PEOPLE TO BUY A PIECE OF SOFTWARE TO PUT ON THEIR PHONE.
WE LOOK AT REALLY WHAT'S AFFECTING THEIR POCKET.
WHERE PEOPLE LOSE MONEY.
FOR US IT'S MORE IMPORTANT TO LOOK AT SITUATIONS WHERE PEOPLE MIGHT FIND THEY'RE RESPONDING ABOUT SMS AND SIGNING UP TO PREMIUM RATES SERVICE AND LOSING 20, $30 A MONTH THAN ONE THAT'S AN EXPLOIT AND THE FACT YOU CAN GO ONTO E BAY WITH WARE INSTALLED AND TRACK THEIR PHONES FOR US COME INTO THE OVERALL UMBRELLA OF SECURITY THREATS WE NEED TO LOOK AT AS AN INDUSTRY.
>> HOW DOES ADAPTIVE MOBILE

IDENTIFY THOSE THREATS.
>> BECAUSE WE SIT WITHIN AN OPERATORS NETWORK WE'RE PROCESSING ABOUT 28 BILLION EVENTS, SMS WEB REQUESTS.
ONE OF THE KEY FOR US AND WE OFTEN HERE REPORTS ABOUT HOW FAST ANDROID IS GROWING.
65% UPTAKE IN MALWARE APPS, ANDROID VIRUSES ARE ACTUALLY VERY EASY TO WRITE.
MOST OF THEM PEOPLE TAKE A LEGITIMATE APPLICATION OFF A STANDARD APP STORE AND SPEND 25 MINUTES ADDING A ROUTINE INTO IT AND REPACKAGE IT AND THROW IT UP ON THE THIRD.
IF YOU LOOK AT THE NUMBER OF INDIVIDUAL FAMILY VIRUSES THERE ARE 450 FOUND LAST YEAR.
WHAT WE REPORT IN VARIANCE TEND TO BE LOTS OF COPIES OF THE SAME UNDERLYING VIRUS SO WE'RE IN RISK, IN MY VIEW, OF CREATING A HYPE.
NOW IT IS A PROBLEM.
AN INDIVIDUAL GETS INFECTED AND CAN LOSE A LOT OF MONEY BUT WE SEE LOW LEVELS OF ACTUAL INFECTION.
YOU HAVE TO BE VERY CARELESS IN MANY CASES TO BECOME INFECTED SO THERE ARE THINGS THE CONSUMERS CAN DO TO MAKE SURE THEY'RE NOT AT RISK.
>> AND WE'LL CERTAINLY GET TO THOSE BUT I WANTED TO ASK DAN AND PATRICK IN YOUR RESEARCH, HOW ARE YOU DEFINING MOBILE MALWARE.
BOTH OF YOU HAVE LOOKED AT IN THE WILD QUITE A LOT.
WHAT ARE YOU LOOKING FOR.
>> I TAKE A CONSERVATIVE APPROACH AND PUT THE BOUNDARY AT UNAUTHORIZED ACCESS TO DATA IF

IT'S SOMETHING I INSTALLED AND KNOWINGLY OR UNKNOWINGLY GIVEN IT ACCESS IT'S MORE OF A PRIVACY EVERYBODY YOU BUT WHEN IT EXPLOITS A FLAW OUTSIDE OF WHAT I GIVE IT ACCESS TO IS WHAT I DETERMINE A PIECE OF MALWARE.
THE ONES THAT MOST COMMONLY GET EXPLOITED ARE CALLED JAILBREAKS THAT CAN BE USED FOR GOOD AND BAD PURPOSES BUT WITH MALWARE THEY GIVE ACCESS TO THE DATA ON THE PHONE.
MANY OF THE OTHER THREATS OUTSIDE OF THAT AREN'T VERY SPECIFIC TO MOBILE.
THEY ALSO OCCUR ON THE DESK TOP AFTER THEY JUST DIFFERENT IN FLAVOR ON MOBILE DEVICES BECAUSE OF THE DIFFERENCE IN USER INTERFACE SO I'M LESS INTERESTED IN THOSE AND MORE INTERESTED IN THE OUT-BASED ATTACKS PREVALENT ON THE PLATFORMS.
>> SO DAN, YOU'RE LOOKING AT WHAT IT DOES TO DECIDE IF IT'S MALWARE.
>> YEAH.
>> WHAT ABOUT YOU, PATRICK.
>> IN THE INTEREST OF TIME I'M GOING TO SAY I AGREE WITH WHAT'S BEEN SAID AND THE RESEARCH I HAVE TAKES WHAT THE COMMUNITY HAS IN MALWARE AND THERE ARE APP HAS IT DO A LOT FOR YOU BUT REQUIRE A LOT OF PRIVATE INFORMATION.
ARE THEY GOOD AND BAD?
THAT'S IN THE EYE OF THE BEHOLDER.
SO WHEN I TALK ABOUT MALWARE IT'S ABOUT WHAT THE COMMUNITY HAS AGREED IS MALICIOUS.
>> OKAY.
I'D LIKE TO SHIFT THE DISCUSSION TO THE THREAT VECTORS.

OMAR, YOU TOUCHED ON SEVERAL OF THESE AND DAN HAS DONE A LOT OF RESEARCH INTO THE VARIOUS WAYS MALWARE GETS ONTO A DEVICE.
IF YOU WANT TO TALK ABOUT YOUR RESEARCH YOU CAN STEP UP TO THE PODIUM.
>> THE SLIDES ARE JUST UP THERE FOR REFERENCE FOR YOU GUYS.
SO WAS MENTIONED BEEN DAN GUIDO WE UNDERSTAND ATTACKERS MUCH BETTER THAN TODAY TO BUILD MORE EFFECTIVE DEFENSES BASED ON THAT KNOWLEDGE.
RATHER THAN SPECIFICALLY FOCUSSED ON VULNERABILITIES FOR MALWARE WE TEND TO LOOK AT A HIGHER LEVEL AND LOOK AT ATTACKS AND LOOK AT THE GOALS OF THOSE ATTACKS AND HOW ATTACKERS ACHIEVE THEM AND AS A MORE HOLISTIC UNDERSTANDING HELPS EXPLAIN WHY CERTAIN TRENDS ARE COMING ABOUT AND WHY HACKERS ARE GOING AFTER ONE ANGLE OR ANOTHER TO BE PREDICTIVE.
AS HAS BEEN MENTIONED THERE ARE MANY VULNERABILITIES ON MOBILE DEVICE TODAY AND PEOPLE CAN COME UP WITH NEW ONES AS MUCH AS THEY WANT.
YOU CAN TALK ABOUT OTHER APPS AND NFC AND WIRELESS AND BREAKING INTO PHONES AND READ DATA DIRECTLY OFF RADIOS A COUPLE FEET AWAY.
FORTUNATELY, WE DON'T SEE A LOT OF THOSE ATTACKS EXPLOITED IN THE WILD.
INSTEAD WHAT OUR ANALYSIS PROVIDES IS SEPARATING THE POSSIBLE ATTACKS FROM THE PROBABLE ATTACKS.
THE WAY WE DO THAT IS THROUGH THIS ECONOMIC ANALYSIS WHICH IS SIMILAR HOW AN MBA WOULD HELP A

COMPANY DETERMINE TO ENTER A NEW MARKET OR A COMPANY WANTS TO ENTER INTO A NEW MARKET IN CONSUMER GOODS.
THEY'RE NOT CHAOTIC DECISIONS.
THEY'RE DELIBERATE MADE ON BEHALF OF THE ATTACKERS.
WE LOOK AT HOW LARGE IS THE MARKET, HOW LARGE THE NUMBER OF USERS WE CAN TARGET, HOW DO THOSE NUMBERS OF USERS WE CAN TARGET, HOW MANY CAN WE CONVERT TO USERS OF OUR MALWARE AND WHAT ARE THE CONVERSION AND CAPTURE RATE IN THE GIVEN MARKET AND WHAT ARE THE OPERATING EXPENSES TO PERFORM THE ATTACK.
DO WE HAVE THE HUMAN RESOURCES AND TECHNICAL RESOURCES AND HOW MUCH ARE THEY.
A LOT OF PEOPLE THINK OF COST ATTACK IS EASY BUT THERE'S A RISK OF ENFORCEMENT OF JAIL OR REMOVED THE APP STORE AND MAY HAVE AN ESTABLISHED PROCESS THAT MAKES IT CHEAPER.
POTENTIAL REVENUE CAN COME FROM NUMBER OF TARGETS AND THE ABILITY TO MONETIZE IT.
CERTAIN TYPES OF DATA ARE MORE VALUABLE THAN OTHERS.
SO GOING BY THIS KIND OF ECONOMIC ANALYSIS WHAT WE SEE IS THERE ARE BASICALLY FACTORIES SET UP AND BUSINESS PROCESSES BEING ABUSED WITHIN THE MALWARE ECO SYSTEM.
WHEN WE LOOK AT MALWARE TODAY THIS IS THE PATH IT TAKES TO ABUSE DATA ON THE DEVICES.
ALL THE NEW KINDS OF MALWARE YOU HEAR ABOUT MOST THE NEW KINDS OF MALWARE ARE SIMPLE VARIATIONS ON THE SIX STEPS.
FIRST, WE JUST SET UP THE MALWARE.

WE TALKED ABOUT APP REPACKAGING
YOU NEED AN APPLICATION WITH NO
UI AND PROBABLY THE MOST SIMPLE
APPLICATION AND PEOPLE CAN COME
UP WITH THOUSANDS AND THOUSANDS
OF VARIATIONS ON IT IN A SHORT
PERIOD OF TIME AND TAKE THAT TO
A LEGITIMATE APPLICATION OR
LOOKS LIKE ONE AND NOW WE HAVE
ALL OF OUR CAPABILITIES SET UP
AND HAVE SO SCALE IT UP AND PUT
IT ONLINE WHERE OTHER PEOPLE CAN
SEE IT AND DRIVE INSTALLATIONS.
THAT'S WHERE THERE'S VARIANCE.
WE CAN CONVINCE PEOPLE TO
INSTALL THEM THROUGH SMS OR
ADVERTISEMENT ON A WEBSITE, WE
CAN SEND THEM E-MAILS, PUT THEM
IN A LEGITIMATE APP STORE AND
GAIN THE METRICS TO PUSH THEM
HIGHER UP IN POPULARITY RATINGS.
AT THAT POINT WE HAVE
APPLICATIONS OF OUR CREATION ON
PEOPLE'S MOBILE DEVICES.
AT THAT POINT THAT'S WHERE WE
WANT TO START GAINING ACCESS TO
DATA WE NEED AND GETTING IT BACK
TO US.
SO THE PRIMARY WAY WE DO THAT IS
BREAK OUT OF THE APPLICATION
SANDBOX PRESENT ON MOST MOBILE
DEVICES WITH A JAILBREAK.
THEY'RE UNPATCHED FLAWS PRESENT
IN MOBILE DEVICES TO ALLOW ME TO
ACCESS DATA IN ANOTHER
APPLICATION'S SANDBOX.
AFTER WE GAIN ACCESS TO ALL THAT
DATA, WE NEED TO TAKE IT, BUNDLE
IT UP AND SEND IT SOME WHERE
ELSE AND THAT COULD BE A SITE I
SET UP TO JUST STORE
INFORMATION.
AT THAT POINT IT'S JUST ABUSE.
WE HAVE TO TAKE THE DATA AND DO
SOMETHING BAD WITH IT AND THAT'S
A LITTLE OUTSIDE THE SCOPE OF

THIS DISCUSSION.
I LIKE FRAMING THE ATTACKS IN A SYSTEMATIC PROCESS BECAUSE IT'S CLEAR IF WE DISRUPT ONE OF THE STEPS THE PERSON CAN GET TO THE BOTTOM AND ACHIEVE THEIR GOAL.
IF THEY CAN'T PUT THEIR APP ON THE APP STORE AND PUT IT ONLINE AND GET TO THE NEXT STEP WHERE THEY GET YOU TO INSTALL, IF THEY CANT GET YOU TO INSTALL IT YOU

CAN'T RUN IT AND IT FRAMES THE DISCUSSION FOR DEFENSES TO PREVENT THE THREAT AND PREVENT OTHER THREATS WE MAY CARE ABOUT BUT NOT AS MUCH AS THE DOMINANT ONE.
IT'S ALSO NICE BECAUSE IT EVOLVES OUR RESPONSE BEYOND THE VULNERABILITIES AND YOU CAN MITIGATE THE PROCESS THEY'VE SET UP RATHER THAN JUST FOCUS ON PARTICULAR VULNERABILITIES AND LOOK AT WHAT MAKES A VULNERABILITY USEFUL IN THE CONTEXT OF THIS ATTACK PATTERN.
SO KEEPING WITH OUR ECONOMIC ANALYSIS IF YOU'RE IN BUSINESS YOU MAY CALL THIS A VALUE CHAIN, IF YOU'RE IN THE MILITARY YOU MAY CALL IT A KILL CHAIN.
IT'S IDEAS THAT HAVE BEEN ADAPTED FROM OTHER ENVIRONMENTS TO WORK FOR SECURITY.
SO TO USE AN EXAMPLE OF WHY WE SEE CERTAIN ATTACKS AND NOT OTHERS I WANT TO TALK A BIT ABOUT THE WEB.
PEOPLE ARE CONCERNED WITH THE FACT WE HAVE WEB BROWSER EXPLOITS ON DESK TOPS AND THAT'S THE DOMINANT VECTOR THROUGH WHICH DESKTOPS GET COMPROMISE AND THINK MOBILE'S THE SAME THING AND THAT'S NOT YET BEEN

REALIZED AND I'LL SHOW WHY.
FIRST, CONSTRUCT THE ATTACKS TO TAKE OVER THE WEB BROWSER TO EXPLOIT THE WEB BROWSER AND GAIN ACCESS TO ITS SANDBOX AND BREAK OUT AND HERE I HAVE TWITTER AND BANK OF AMERICA BUT IT CAN BE ANY APP.
WE NEED TO CONSTRUCT A CHAIN OF EVENTS TO MAKE IT HAPPEN.
WE NEED TO CHANGE HOW WE CHANGE THE MALWARE AND PUT IT ONLINE AND THEY'RE NEW PROCESSES I NEED TO SET UP AS AN ATTACKER WITH A COST ASSOCIATED WITH IT AND NEED HUMAN RESOURCES WITH SKILLS TO BE ABLE TO DO.
IT MAY AFFECT MY OPERATING COST IN A PROHIBITIVE WAY.
WHEN WE AT THE MOBILE MALWARE COMMUNITY AND ASK DO THEY HAVE THE SKILLS TO WRITE THINGS TO TAKE OVER THE BROWSER, OVERWHELMINGLY THE ANSWER HAS BEEN NO AND THEY'RE USING CODE ESTABLISHED ONLINE BY OTHER SMARTER PEOPLE OUTSIDE MAYBE IN THE SECURITY INDUSTRY THAT DON'T HAVE MALICIOUS INTENT AND NO ONE'S PUBLISHING TO THE CODE AND HAVE SO SET UP THE INFRASTRUCTURE TO LAUNCH THESE THINGS AND CONSTRUCT A PROCESS THAT ABUSES THEM.
SO HOW DOES IT AFFECT MY MARKET SIZE?
WELL, IF I'M FACEBOOK OR I'M A NORMAL MOBILE -- IF I'M A NORMAL COMPANY THAT WANTS TO GAIN ACCESS TO MOBILE DEVICES LIKE FACEBOOK THE DECISION MAKING I GO THROUGH IS I CAN SET UP A MOBILE WEBSITE OR MAKE AN APP AND LEGITIMATE COMPANIES DECIDE TO MAKE APPS BECAUSE IT'S A MORE EFFECTIVE WAY TO GET EYEBALLS ON

A MOBILE DEVICE.
THE WEB BROWSER PERSPECTIVE IS A SMALLER MARKET AND SLIGHTLY HARDER TO REACH THESE PEOPLE BECAUSE THE ADVERTISING MECHANISMS THAT GIVE ME ACCESS TO ALL THESE POPULAR WEBSITES ARE HARDER TO GET INTO.
THEY'RE MORE EXPENSIVE AND LESS ADVERTISEMENTS PRESENT ON MOBILE WEBSITES AND THAT SORT OF THING.
SO IT'S HARDER ALSO BECAUSE WHEN WE'RE LOOKING AT MOBILE BROWSERS, I GUESS I SHOULD EXPLAIN THE SLIDE, SHOULDN'T I.
WHEN WE LOOK AT MOBILE BROWSERS WE FIRST HAVE TO EXPLOIT THE WEB BROWSER AND FROM THE BROWSER WE NEED TO BREAKOUT OF THE SANDBOX INSIDE TO ACCESS OTHER APPLICATIONS.
NOW I'VE DOUBLED BY OPERATING COSTS.
I NEED TWO EXPLOITS INSTEAD OF GIST ONE.
-- JUST ONE.
SO I'M SAYING WEB EXPLOITS ARE POSSIBLE AND PEOPLE CAN PROVE THAT TO YOU AT ANY SECURITY CONFERENCE BUT ARE THEY PROBABLE?
I'M GOING TO SAY PROBABLY NOT BECAUSE THE PROCESS TO TAKE ADVANTAGE OF THESE THINGS ARE NOT SET UP AND THE SKILLS TO PERFORM THESE ATTACKS ARE NOT WIDESPREAD.
SO WE HAVE A VERY CONSERVATIVE ESTIMATE AROUND THE DEVELOPMENT OF MOBILE MALWARE WE THINK IT WILL BE ABCENTRIC FOR A WHILE AND WHEN WE THINK OF THE MOBILE COMMUNITY WE THINK OF IT AS DELIBERATE AND SLOW AND THEY'RE NOT QUITE DOING A LOT OF INNOVATION.

THEY'RE LOOKING AT BUSINESS PATTERNS AND SCALE TO PROFIT OFF EFFECTIVELY OR REPEATED.
AND THAT'S ALL I HAVE TO SAY.
>> YOU'RE NOT DONE YET.
YOU CAN HAVE A SEAT BUT I HAVE SOME QUESTIONS FOR YOU.
WE HAVE ALL SEEN BATMAN MOVIES AND KNOW THERE ARE BAD ACTORS OUT THERE NOT MOTIVATED BY PROFIT BUT BY POLITICAL MOTIVES OR SOMETHING ELSE.
YOUR ARGUMENT SEEMS TO BE WE SHOULD FOCUS OUR EFFORTS FROM AN ECONOMIC PERSPECTIVE WHAT'S MOST LIKELY TO HAPPEN.
AND WOULD IT BE APPROPRIATE FOR SECURITY COMPANIES TO IGNORE THE CRAZY BAD ACTOR WHO CAN DO SOMETHING BAD.
>> LIKE THE ELEPHANT IN THE ROOM IS ANONYMOUS.
THEY'RE NOT USUALLY VERY SOPHISTICATED AND HAVE TOOLS THAT CAN BE DISTRIBUTED ON A WIDE SCALE SO NON-TECHNICAL PEOPLE CAN PERFORM THE ATTACKS AND AID THESE KIND OF DENIAL OF SERVICE ATTACKS.
I LIKEN IT TO AN OPEN-SOURCE SCENARIO WHERE A COUPLE YEARS AGO WE THOUGHT IT WOULD TAKE OVER THE WORLD AND BE A THREAT TO ALL COMMERCIAL SOFTWARE BUT IT DEPENDS ON PEOPLE'S FREE TIME TO ADD TO THIS KIND OF DEVELOPMENT.
YOU HAVE TO HAVE A VERY CHARASMATIC PERSONALITY TO CONVINCE ALL THESE PEOPLE TO GIVE UP THEIR TIME AND CONTRIBUTE IT TO YOUR PROJECT AND MAKE IT SUCCESSFUL.
WE HAVEN'T REALLY SEEN A LOT OF THE PURE-OPEN SOURCE TAKE OVER AND IT'S THE SAME KIND OF THING

WITH THREATS LIKE ANONYMOUS AND OTHER PEOPLE NOT FINANCIALLY MOTIVATED.
THEY HAVE LESS INCENTIVE TO CONSTRUCT THE ELABORATE AND SOPHISTICATED, HIGHLY-RELIABLE ATTACK PATTERNS OTHER GROUPS DO.
THE KINDS OF THINGS I SEE FROM PEOPLE THAT ARE NOT FINANCIALLY MOTIVATED TEND NOT TO BE VERY SOPHISTICATED OR MUCH OF A THREAT AT ALL.
>> ARE YOU SEEING ATTACKS THAT FALL INTO THIS CATEGORY OF MAYBE NOT FINANCIALLY MOTIVATED AND DO YOUR PRODUCTS PROTECT AGAINST THOSE?
ARE YOU LOOKING FOR THEM?
ARE YOU FINDING THEM?
ARE THEY OUT THERE?
>> THE BIG QUESTION FOR ALL CARRIERS IS DO WE HAVE MOBILE BOTNETS AND HOW DO YOU DETECT THEM AND WHO'S RUNNING THEM?
BOTNETS ARE THERE AND SOME ARE BEING USED FOR FINANCIAL GAIN.
THERE ARE OTHERS WE DETECTED AND YOU CAN'T SEE AN IMMEDIATE FINANCIAL RETURN FROM THEM.
IT COULD BE IT'S JUST A BADLY SET UP ORGANIZATION WHO HASN'T QUITE GOT THEIR BUSINESS MODEL RIGHT SO MISSING THE OPPORTUNITY TO MAKE MONEY.
BUT THERE ARE SITUATIONS WHERE WE'VE SEEN DEVICES UNDER THE CONTROL OF SERVICES IN OTHER COUNTRIES.
SO FROM A CRITICAL INFRASTRUCTURE AND PROTECTION PERSPECTIVE YOU LOOK AT THOSE IN MORE DETAILS AND START TO UNDERSTAND, WELL, IF YOU HAVE MOBILE DEVICES SITTING ON A NETWORK WAITING FOR COMMANDS FROM CHINA OR SERVERS IN

SOUTHEAST ASIA, FOR EXAMPLE, AT
WHAT POINT CAN THEY BE USED AND
WHAT CAN THEY BE USED FOR.
>> I AGREE WITH THAT.
I THINK HAVE WE SEEN ATTACKS
THAT ARE NOT FINANCIALLY
MOTIVATED, YES.
THE MOST DRAMATIC DECREASE WE
SAW WAS PROBABLY INITIALLY
STARTED AND SPEAKS TO THE
EVOLUTION AS WELL AS THE LACK OF
SOPHISTICATION THE HIGHEST
INSTANCE AT ONE POINT WAS TAKEN
THE CONCEPT OF TROJAN HORSES BUT
IT'S BEING MUCH MORE MOTIVATED
NOW BY FINANCIAL GAIN OR GAININGDO WITH
THE FACT THAT IT'S NOT JUST A
SINGLE COLLECTION EFFORT THAT
CAN BE MONETIZED.
OFTENTIMES IT'S A MULTIPRONGED
EFFORT THAT HAS TO TAKE PLACE TO
BE ABLE TO CREATE SOMETHING FROM
EITHER A SERVICE PERSPECTIVE OR
DATA DUMP COLLECTED ENOUGH
PERSONAL INFORMATION THAT CAN
MONETIZE ON THE BLACK MARKET.
IT TAKES SOME COLLECTION EFFORT
AND SOME SOCIAL ENGINEERING
EFFORT AS WELL.
SO YES, DO WE PROTECT AGAINST
IT?
I AGREE WITH THE PANELISTS, I
THINK WHERE THE INDUSTRIES
HEADED AS WELL AS WHERE THE
MAJORITY OF THE EFFORT IF NOT
MORE OF THE SOPHISTICATION IS
GOING IS MORE TOWARDS
FINANCIALLY MOTIVATED ATTACKS.
>> OKAY.
SO I WAS READING LAST NIGHT SOME
COLLEAGUES OF PATRICK'S AT
GEORGIA TECH HAVE CREATED AN
iPHONE CHARGER THAT CAN INJECT
MALWARE IN TO A PHONE WHEN IT'S
BEING CHARGED.
AND I THINK WE'RE GOING HEAR

MORE DETAILS ABOUT THIS AT THE
BLACK HACK CONFERENCE.
ARE THESE TYPES OF INFECTIONS
SOMETHING THAT OMAR, YOUR
SECURITY PRODUCT COULD ACTUALLY
PROTECT AGAINST AS WELL?
HOW WOULD YOU KNOW A DEVICE WAS
INFECTED THROUGH HARDWARE?
IS THAT SOMETHING THAT'S KIND
OF, THERE ISN'T A PROTECTION
AGAINST THAT AT THIS POINT?
>> IN TERMS OF INCURSION ITSELF,
YOU KNOW, THAT'S NOT SOMETHING
THAT WE WOULD NECESSARILY
IDENTIFY WHETHER IT CAME FROM,
YOU KNOW, THROUGH USB OR WHETHER
IT CAME THROUGH A WEB-BASED OR
IP CONNECTION, ET CETERA.
IT'S REALLY AS AN END POINT
SECURITY COMPANY WE'RE LOOKING
FOR ONCE THE PAYLOAD HAS EITHER
BEEN DELIVERED COMPARING IT TO
WHAT IS NONE TO BE MALICIOUS
PAYLOAD OR MALICIOUS SOFTWARE
ATTACK OR IF USER IS HEADED OFF
IN TO A WEB ENVIRONMENT, AGAIN,
I AGREE WITH DAN THAT HIJACKING
A MOBILE BROWSER ISN'T WHAT'S
HAPPENING.
IT'S MORE PHISHING ATTACKS.
IT'S MORE DELIVERY METHOD.
A LOT OF IT HAS TO DO WITH
EDUCATION TO THE CONSUMER OF
TURNING OFF WiFi, TURNING OFF
BLUE TOOTH WHEN YOU'RE NOT USING
IT AS WELL AS TEACHING FOLKS THE
SAFETY OF CONNECTING TO VARIOUS
THIRD PARTY SOURCES.
THOSE ARE SOME OF THE THINGS
FROM A CONSUMER EDUCATION
PERSPECTIVE ARE PARAMOUNT AS
WELL.
NO, NOT NECESSARILY WHAT PRATT
PARTICULAR'S COLLEAGUES HAVE
DONE.
>> I WANT TO ADD SOMETHING.

I THINK WE'RE LEAVING OUT, VERY FOCUSED ON MOBILE DEVICE BUT IF WE TALK ABOUT AN ADVERSARY WHO MAY OR MAY NOT HAVE A FINANCIAL INTEREST, SAY A STATE ACT TO, WE HAVEN'T TALKED ABOUT NETWORKS AT ALL.
NETWORKS ARE FULL OF VULNERABLE UNAUTHENTICATED PROTOCOLS F THAT'S THE ADVERSARY WE'RE WORRIED ABOUT, I DON'T SEE A STATE ACTOR NECESSARILY TRYING TO SHUT DOWN THE NETWORK BY SHUTTING DOWN A HUGE NUMBER OF DEVICES WITH A SINGLE DEVICE, TALK TO SPECIFIC MODES IN THE NETWORK AND SHUT DOWN TRAFFIC.
YOU KNOW, I THINK WE NEED TO BE SURE WE CONSIDER THE NETWORK ASPECTS AS WELL AS THE DEVICES.
>> RIGHT.
GARETH, IS THAT WHERE YOU COME IN?
>> COMPLETELY AGREE.
FROM A NETWORK PERSPECTIVE, YOU ACTUALLY DON'T CARE WHETHER AN APPLICATION WAS FROM MALICIOUS PURPOSES OR BADLY WRITTEN.
SOMETHING WHICH JUST SITS ON THE NETWORK AND STARTS TO, IS TOO CHATTY, SENDS TOO MANY REQUESTS THROUGH THE CELL TOWERS CAN HAVE AS MUCH OF A PROBLEM FOR AN OPERATOR AS SOMETHING WHICH IS DESIGNED TO ACTUALLY CAUSE PROBLEMS ITSELF.
SO AN OPERATOR IS ALWAYS CONCERNED ABOUT THE FACT THAT ANY APPLICATION COULD POTENTIALLY USE UP ALL OF THE RESOURCES WITHIN A PARTICULAR LOCATION.
IF THAT WAS IN DOWNTOWN D.C., IT WOULD START TO HAVE A MAJOR IMPACT ON THE REVENUE FOR THAT PARTICULAR CARRIER.

>> PATRICK, YOU PROVIDED A
PERFECT SEGUE TO YOUR OWN
PRESENTATION.
MAYBE WE'LL HEAR FROM YOU NOW.
>> FUNNY HOW THAT WORKS OUT.
.
>> I WANT TO START OFF BY
TELLING YOU A STORY ABOUT WHY
IT'S WONDERFUL TO BE A
PROFESSOR.
THAT'S ONE OF THE REALLY GREAT
THINGS IS THAT I CAN HAVE
RANDOM, ARBITRARY PROJECTS, AN
ARMY OF STUDENTS WHO WILL HELP
ME DO THOSE THINGS.
LET ME TELL YOU ABOUT THEM.
SO A COUPLE MONTHS AGO I STORMED
IN TO MY LAB AND I SAID EVERYONE
DROP WHAT YOU'RE DOING, NEXT 30
MINUTES I WANT YOU TO FIND THE
MOST OUTRAGEOUS NEWS STORIES YOU
CAN POSSIBLY FIND.
THAT'S THE JOB, COME BACK TO ME
IN 30 MINUTES.
WE GOT BACK TOGETHER.
THE STUDENTS PROVIDED ME THINGS
BETTER THAN I COULD HAVE HOPED
FOR.
TURNS OUT THE HIGHEST NUMBER OF
BIG FOOT SIGHTINGS OCCUR IN
OHIO.
IF YOU ASK LOCAL POLICE IN
SCOTLAND, THE LOCHNESS MONSTER,
ABSOLUTELY REAL.
IN FACT IF YOU'RE FROM THE WEST
COAST, WE CAN LAUGH AT THIS OF
COURSE BECAUSE THESE ARE
EXTRAORDINARY CLAIMS, REQUIRE
ABSOLUTELY EXTRAORDINARY DATA TO
SUPPORT THEM.
WE DON'T HAVE THAT DATA.
SO WE LAUGH.
SO THE NEXT PART OF THE
ASSIGNMENT WAS OKAY, I WANT YOU
TO GO OUT AND LOOK FOR STORIES
RELATED TO YOUR RESEARCH, HAVE

SIMILARLY LARGE CLAIMS THAT WE CAN'T NECESSARILY ADDRESS.
THEY CAME BACK WITH HEADLINES YOU'VE HEARD.
ANDROID MALWARE EXPLODING 1200% THIS YEAR.
MY FAVORITE ARTICLE WAS THAT ANDROID HAS BECOME THE ULTIMATE PLATFORM FOR MALWARE.
IMAGINE THIS.
AS BAD AS WINDOWS 98 WAS, WE HAVEN'T LEARNED ANYTHING OVER A DECADE SINCE THEN, ANDROID FAR WORSE.
HERE'S WHERE THE COGNITIVE DISDANCE COMES, I DON'T KNOW ANYONE EFFECTED.
WHEN I TALK TO COMPANIES, I KNEW A FRIEND OF A FRIEND OF A FRIEND WHO WAS INFECTED.
SO HOW CAN I PROVIDE PEOPLE WITH GOOD ADVICE WHEN I CAN'T REALLY MEASURE THE PROBLEM?
HOW DO I KNOW WE'RE DOING BETTER WITHOUT MEASURING?
THAT'S WHAT WE AT GEORGIA TECH SET OUT TO DO.
PARTNERED WITH MAJOR CELLULAR ISP IN THE U.S., ASKED TO REMAIN NAMELESS, ABOUT HALF OF YOU IN THE ROOM ARE PROBABLY CUSTOMERS.
AND WHAT WE DID WAS WE SAT AT THEIR DNS RESOLVER AND WATCHED TRAFFIC FOR ABOUT THREE MONTHS.
IF YOU'RE NOT FAMILIAR WITH DNS, WHAT TURNS CNN.COM IN TO AN IP ADDRESS.
WE KNOW A LOT ABOUT DNS AS A MEANS OF IDENTIFYING MALICIOUS DOMAINS, HOSTS, AND SO WHEN A COUPLE OF INTERESTING FINDINGS I WOULD LIKE TO SHARE WITH YOU.
AS A PROFESSOR I HAVE A COUPLE GRAPHS AND NUMBERS BUT I'LL HIT THE HIGH POINTS AS QUICKLY AS I CAN.

THE FIRST THING IS, SO WHAT IS
THIS MOBILE WEB?
WHAT ARE THESE APPS?
WHAT ARE PEOPLE'S BROWSERS
TALKING TO?
WHEN WE COMPARED THE HOSTS THAT
WERE HOSTING THESE APPS AND SO
FORTH, TURNS OUT THAT WE SEE
ALMOST 99% OF THOSE HOSTS IN
TRADITIONAL WIRED ISPs.
WHICH MEANS THAT ALL REPUTATION
DATA THAT SCIENTISTS LIKE MYSELF
SPENT CAREERS AMASSING AND MANY
COMPANIES AS WELL, USE TO REASON
ABOUT MALICIOUSNESS.
GREAT, THE MOBILE WEB IS THE
WEB.
IT'S NOT TERRIBLY SURPRISING OF
COURSE THAT PEOPLE WHO HAVE WEB
PAGES REUSE MANY SERVERS TO
SUPPORT THEIR MOBILE APPS.
THE SECOND IS THIS: DID WE
ACTUALLY SEE MOBILE MALWARE?
MOBILE MALWARE IN GENERAL WILL
RESOLVE SOME DOMAINS OR SOME
HOSTS SO KNOWS WHO IT SHOULD
TALK TO.
EVEN MOBILE MALWARE THAT'S
INVOLVED IN SMS PREMIUM NUMBER
STANDS, IT WILL ON SAY HEY, ARE
WE STILL USING THIS SHORT CODE
TO RIP PEOPLE OFF?
THE RESPONSE WILL COME BACK YES,
WE ARE.
THEN IT WILL SEND OFF THE
MESSAGE.
SO WE WENT AND OPENED UP ALL OF
THE MOBILE MALWARE THAT WAS
AVAILABLE TO THE COMMUNITY A
YEAR AGO, ALSO THEN WENT TO
ANTIVIRUS PROVIDERS AND SAID
TELL US THE DOMAINS, HOSTS THAT
YOU'VE EXTRACTED FROM MOBILE
MALWARE.
THAT WAY WE CAN GET COMMUNITY
CONSENSUS ON WHAT'S MALICIOUS,

WHERE IT'S TALKING TO.
HERE'S WHAT WE SAW.
WE ACTUALLY SAW MOBILE MALWARE AT WORK.
YOU CAN SEE FOR SOME OF THESE FOR EXAMPLE WE SAW A FEW THOUSAND DEVICES, FIVE, 6,000 DEVICES INFECTED DURING OUR THREE MONTH STUDY.
THAT'S BAD, EXCEPT FOR WHEN YOU PUT IT IN TO CONTEXT.
OVER THE COURSE OF OUR STUDY IT TURNS OUT THAT LESS THAN 1/111stth WERE EFFECTED WITH WHAT THE COMMUNITY AGREES IS MOBILE MALWARE, MALICIOUS APPLICATIONS, TO PUT THAT IN TO CONTEXT, THE NATIONAL WEATHER BUREAU, I APOLOGIZE, SAYS THAT THE CHANCES OF BEING STRUCK BY LIGHTNING OVER THE COURSE OF YOUR LIFETIME ARE 1 IN 10,000.
SO DURING THE COURSE OF THIS STUDY YOU WOULD BE FAR MORE LIKELY TO HAVE BEEN STRUCK BY LIGHTNING THAN INFECTED WITH MOBILE MALWARE.
THAT'S NOT THE END OF THE STORY, THOUGH.
WE LOOKED AT ALL THAT REPUTATION INFORMATION THAT WE HAD AND IT TURNS OUT THAT MOBILE DEVICES ARE TALKING TO SIGNIFICANT NUMBER OF MALICIOUS HOSTS.
THE COLUMN I WANT TO YOU CARE ABOUT IS THE MIDDLE ONE, THESE 8% NUMBERS.
I BREAK OUT iOS SEPARATE FROM OTHERS BUT I GIVE YOU A BREAKDOWN, ALL ROUGHLY END UP AT 8%.
WE SHOW THE FOLLOWING.
THAT 8% OF ALL DEVICES IN EACH POPULATION HERE IN iOS USER, ANDROID USER, WINDOWS MOBILE USER, GO AND TALK TO KNOWN

MALICIOUS SERVERS.
SERVERS THAT WE DON'T HAVE
INFORMATION ON IN TERMS OF
MOBILE MALWARE.
SO THE THOUGHT THAT iOS IS
SOMEHOW MAGICALLY SAFER THAN ANY
OTHER DEVICE OR THAT ANDROID IS
SOMEHOW AUTOMATICALLY WORSE THAN
ANY OTHER DEVICE, DON'T STAND UP
TO OUR ANALYSIS FROM THE NETWORK
PERSPECTIVE.
SO I WANT TO FINISH MY TIME HERE
WITH THE FOLLOWING MUCH.
I'M NOT SAYING THAT
MALICIOUSNESS IS IMPOSSIBLE.
I'M SAYING THAT FOR ALL OF THE
DOWNLOADS, FOR ALL OF THE
VARIANCE PEOPLE SAY WE'RE SEEING
FROM THE NETWORK PERSPECTIVE WE
DON'T SEE INFECTION HAPPENING
ALL THAT OFTEN.
IF WOULD YOU LIKE TO KNOW MORE
DETAILS OF COURSE, I'M AVAILABLE
AFTER THIS.
AND THE PAPER IN OUR METHODOLOGY
ARE PUBLIC.
I ENCOURAGE TO YOU TAKE A LOOK
AT THAT AND JUDGE OUR MEASURES.
THANK YOU.
OMAR, I THINK NQ'S ESTIMATE WAS
SOMETHING LIKE 2% OF DEVICES IN
THE U.S. ARE INFECTED.
THIS WAS NOT IN YOUR
PRESENTATION BUT I THINK WHEN WE
SPOKE EARLIER THAT WAS THE
ESTIMATE YOU GAVE ME.
HOW DO YOU EXPLAIN THE
DIFFERENCE BETWEEN THAT
STATISTIC OR YOU CAN GIVE ME A
DIFFERENT STATISTIC, I DON'T
WANT TO PUT WORDS IN YOUR MOUTH,
BETWEEN THAT STATISTIC AND THE
NUMBERS THAT PATRICK IS SEEING
IN HIS RESEARCH?
>> THOSE ARE, THE STATISTIC YOU
MENTIONED IS CORRECT.

THAT IS WHAT WE'RE SEEING WITHIN THE ENVIRONMENT.
AND THE PREVALENCE RATE IS SIGNIFICANTLY HIGHER OUTSIDE THE U.S. THAN IT IS IN THE U.S.
BUT THE INFECTION RATES WE'RE SEEING VERSUS THE LIBRARIES WE MAINTAIN ARE ON THAT ORDER.
OBVIOUSLY PRIMARILY ON, WITHIN THE NETWORK DEVICES TODAY, BUT THE REASON WE'RE ALSO SEEING IT SPECIFICALLY IS BECAUSE I THINK THE FRAGMENTATION OF OPEN RATING SYSTEMS, FRAGMENTATION OF UPDATES THAT WAS MENTIONED EARLIER CREATES SOME VULNERABILITIES.
WE'LL DEFINITELY FOLLOW UP WITH PATRICK AND HIS TEAM ON COLLABORATING ON THE LIBRARIES AND MAKING SURE THAT THE DATA CORRELATES.
BUT FROM OUR PERSPECTIVE, 8 FIGURES, SO TREMENDOUS AMOUNT OF DATA COMING IN AROUND WHAT THE INFECTION RATESR I WOULD AGREE GENERALLY THE PROPAGATION RATES ARE FAIRLY LOW.
SO WHEN WE DO SEE, EVEN THE 600,000 UNIT ATTACK THAT WE SAW HAPPEN IN THE ASIAN MARKET, SIGNIFICANT, BY AND LARGE, FAR AND AWAY THE LARGEST INFECTION RATE.
GENERALLY INFECTION RATES ARE LOWER.
THEY DON'T PROPAGATE AS QUICKLY.
AND THE INTANSES ARE SIGNIFICANTLY, INSTANCES FOCUSSED ON MARKETS WHERE THIRD PARTY APPLICATION MARKETPLACES ARE A SOURCE OF DISTRIBUTION.
IF YOU WERE TO WALK AROUND THIS ROOM OR JUST DO A SHOW OF HANDS OF FOLKS WHO HAVE iOS OR ANDROID WHO PERFORMED INSTALLATION

OUTSIDE OF GOOGLE PLAY OR
OUTSIDE OF iTUNES APP STORE,
PROBABLY VERY LOW.
HOW MANY INSTALLED AN
APPLICATION OUTSIDE OF iOS,
iTUNES OR GOOGLE PLAY?
>> OUTSIDE OF THE INDUSTRY THAT
WE'RE IN, RIGHT?
>> PUT YOUR HAND DOWN IF YOU'RE
A TECHNICAL EXPERT OR ON A PANEL
TODAY.
>> DON'T ADMIT IF IT YOU'RE FROM
THE ST C.
>> STATISTICS PROFESSORS WOULD
BE UPSET ABOUT SAMPLING ERROR
HERE.
>> IT'S PROBABLY A CUREATED
SAMPLE HERE.
IT SPEAKS TO THE FACT THAT THE
INSTANCES OF THIRD PARTY APP
DOWNLOADS, THIRD PARTY
MARKETPLACE DOWNLOADS ARE
SIGNIFICANTLY HIGHER OUTSIDE THE
U.S.
DOESN'T MEAN WE'RE IMMUNE HERE
BUT WE'LL FOLLOW UP.
2% IS THE RIGHT NUMBER BASED ON
OUR NETWORKS STATISTICS.
>> ONE THING I WANT TO ADD TO
THIS IS I THINK THE PICTURE OF
THIRD PARTY APPS OR THIRD PARTY
MARKETS AS SORT OF ALWAYS
POLLUTED, ALWAYS BAD IS
CHANGING.
TWO YEARS AGO I THINK THAT THIS
WAS VERY MUCH THE CASE.
BUT THIRD PARTY APP STORES
REALIZE THAT THEY WOULD LIKE TO
MAKE MONEY TOO.
YOU CAN'T MAKE MONEY, OR IT'S
HARDER TO MAKE MONEY AS
LEGITIMATE APP STORE IF YOU'RE
KNOWN FOR HOSTING MALWARE.
MANY WE LOOKED AT HAVE, SINCE
OUR INITIAL STUDIES, PARTNERED
WITH SOME OF THE BIG AV

COMPANIES, REALLY TRIED TO CLEAN OUT THEIR MARKETS.
SO I THINK THE PICTURE IS CHANGING.
>> BY THE WAY, THE WHOLE CONCEPT OF MARKETPLACE REALLY CHANGES THIS SPACE.
I THINK IT'S ACTUALLY SIGNIFICANTLY MORE DIFFICULT TO INFECT USER DEVICE IFS YOU'RE ONE APP IN A SEA OF A MILLION OTHERS.
HOW DO YOU PULL PEOPLE IN WITHOUT ATTRACTING THE ATTENTION OF GOOGLE OR WHOEVER IS, YOU KNOW, DOING THE AUDITING OF THE THIRD PARTY MARKET WITHOUT ADVERTISING?
IF I KNOW HOW TO WRITE AN APP THAT WAS GOING TO GET 10 MILLION USERS, I COULD PROBABLY COME UP WITH A BETTER WAY TO MONETIZE IT THAN STEAL THEIR DATA.
I WOULD LIKE TO REMAIN IN THE APPTOR LONG ENOUGH TO MAKE SOME REAL MONEY.
APP STORE LONG ENOUGH TO MAKE MORE MONEY.
I THINK IT CHANGES THE SPACE PRETTY SIGNIFICANTLY.
>> SORRY, I WANT TO SAY THAT THAT'S NOT THE SAY PEOPLE LIKE JOHN OBERHEIDE CAN'T GETS LOTS OF MALICIOUS APPS IN THE MARKET.
JUST THAT THEY DON'T LAST FOR VERY LONG OR THEY GET BLACK LISTED.
.
>> APP STORE SCANNING IS DEFINITELY, HAS BEEN IMPLEMENTED.
I THE APP STORES ARE CLEANING UP, SEEING THE SAME THING.
WE'RE ALSO SEEING A RISE FROM DISTRIBUTION DIRECTLY FROM SERVERS AS WELL.

THE CONCEPT OF THAT BEING
REPLACED IS DEFINITELY HAPPENING
OUT THERE.
>> THAT KIND OF ANALYSIS LEADS
TO YOU THINK A LOT OF MALWARE IS
THAT IS INCREDIBLY MALICIOUS IS
BURSTING IN NATURE, COMES
QUICKLY AND GOES AWAY.
IT COULD BE HISTORICAL DATA
DOESN'T OVERLAP EXACTLY WITH THE
PERIOD OF BURSTINESS OF THE
MALWARE YOU'RE LOOKING AT?
>> THE GREAT THING ABOUT THIS IS
THAT ALL OF OUR METHODOLOGY IS
PUBLIC.
I WILL POINT TO THE PAPER, THE
ANSWER IS OF COURSE IT IS.
>> OKAY.
JUST CHECKING.
>> COMING BACK ON THE POINT
ABOUT ADVERTISING, TO ALMOST
POINT, WE'RE SEEING A LARGE
GROWTH IN TERMS OF DIRECTLY
LINKED MALWARE.
MALWARE WHICH HASN'T BEEN HOSTED
ON WELL-KNOWN THIRD PARTY APP
STORES.
REMEMBER OUTSIDE OF NORTH
AMERICA, THE MAJORITY OF USERS
WILL GO TO THIRD PARTY APP
STORES.
AS AN EXAMPLE, A RUSSIAN MALWARE
GROUP IN MARCH THIS YEAR PUSHED
OUT SMS MESSAGES TO OVER 2
MILLION SUBSCRIBERS.
ALL OF WHICH DIRECTING THEM
THROUGH TO ONE OF 98 VARIANTS OF
THE NEW PIECE OF MALWARE, ALL
HOSTED ON SERVERS.
IT WASN'T ON WELL-KNOWN APP
STORES.
SO I THINK PEOPLE ARE REALIZING
THAT APP STORES ARE STARTING TO
BECOME A HARD PLACE TO SET
MALWARE UP.
BUT MEANS WE'RE SEEING LOTS OF

PEOPLE PROMOTED THROUGH LINKS
AND GAMES, THROUGH SMS THROUGH
TO PHONES, AND PEOPLE JUST HAVE
TO CLICK ON THAT AND IMMEDIATELY
START TO DOWNLOAD F IT ALREADY
GIVEN APPROVAL TO DOWNLOAD
THINGS FROM THIRD PARTY STORES,
OR OFFMARKET SITES, THEY REMOVED
THAT ONE KEY PIECE OF PROTECTION
THAT THEY HAVE ON THEIR DEVICE.
>> DAN, DO YOU AGREE THAT THAT
--
>> THAT FITS THE PATTERN.
IT'S JUST WHEN WE LOOK AT THE
STEP, YOU KNOW, WHEN WE WANT TO
TAKE THE APP, PUT IT ONLINE, WE
CAN PUT IT ON OUR OWN SERVER,
PUT IT ON THIRD PARTY APP STORE
OR FIRST PARTY APP STORE EFFECTS
HOW MANY PEOPLE YOU CAN
POTENTIALLY REACH.
YOU CAN STILL ADVERTISE
SOMETHING ON FIRST PARTY APP
STORE WITH SMS, PROBABLY HAVE A
LARGER MARKET THAT WAY BECAUSE
YOU'LL GET ADDITIONAL
INSTALLATIONS THROUGH OTHER
MEANS, THROUGH PEOPLE JUST
DOWNLOADING IT BECAUSE THEY SEE
IT BECOMING POPULAR.
BUT ALL THREE OF THOSE ARE
ESSENTIALLY EQUIVALENT.
ALSO SPEAKS TO CONSUMER
BEHAVIOR.
BECAUSE IN THE U.S. WE'RE NOT AS
PRONE TO SMS MARKETS, LAND IN
MEXICO, THE INSTANCE OF SMS
MARKETING IS SIGNIFICANTLY
HIGHER THAN IN THE U.S.
I THINK THAT THE RECEPTIVITY AS
WELL AS LIKELIHOOD FOR CONSUMER
TO CLICK THROUGH ON SMS BASED
MARKETING SCAM, WHATEVER IT
MIGHT BE IN TERMS OF ATTACK,
INITIATED MUCH HIGHER IN MARKETS
OUTSIDE WESTERN EUROPE AND

OUTSIDE THE U.S. THAN IT IS
HERE.
>> I HAVE TO DISAGREE WITH THAT.
THE U.S. IS THE BIGGEST SOURCE
OF SMS SPAM NOT JUST FOR
AMERICANS BUT FOR OTHER
COUNTRIES AROUND THE WORLD.
>> I DIDN'T MEAN THE LOCATION,
BUT THE SPECIFICALLY USERS
CLICKING THROUGH.
>> WE'RE THE SOURCE BUT NOT
CONSUMING IT.
>> YEAH, YEAH.
>> BE PROUD OF THAT.
>> YOU'RE ABSOLUTELY RIGHT.
WE SEE TREMENDOUS SOURCES COMING
FROM THE U.S. BUT IN TERMS OF
CONSUMER BEHAVIORS,
CLICK-THROUGHS, INCIDENT RATES
ARE HIGHER IN MARKETS OUTSIDE
THE U.S.
>> SO PATRICK, YOU SAID THAT
OVER 8% OF PEOPLE IN THE U.S.
ARE VISITING THESE MALICIOUS
SITES BUT INFECTION RATE IS
INCREDIBLY LOW.
WE TALK ABOUT AS CONSUMERS WERE
A LITTLE BETTER EDUCATED MAYBE
AREN'T CLICKING ON THINGS.
8% OF PEOPLE CLICKING ON THINGS
AREN'T GETTING INFECTED.
WHAT IS THE REASON FOR THAT?
>> SO I SHOULD ADD THROUGH
CAVEAT, THE FIRST IS BECAUSE WE
LOOK FROM DNS I CAN'T TELL YOU
IF THEY CLICKED ON IT OR HOW
THEY GOT THERE, JUST THAT THEY
GOT THERE.
I ACTUALLY FIND THIS SORT OF
ENCOURAGING.
STRICTLY SPEAKING WITH MY
TECHNICAL HAT ON, THAT IF THE
OPERATING SYSTEMS, OF COURSE
THERE ARE VULNERABILITIES, IF
OPERATING SYSTEMS ARE HARD
ENOUGH TO BREAK, YOU CAN'T DO IT

AUTOMATICALLY WITHOUT HAVING TO TRICK THE USER, BOY, I WISH WE WERE IN THAT SORT OF STANDING IN THE DESKTOP SPACE.
THAT WOULD BE AMAZING.
SO THE FACT THAT MOST, A LOT OF WHAT WE SEE IS VERY MUCH SOCIAL ENGINEERING ORIENTED FROM A TECHNICAL PERSPECTIVE IT MEANS WE'RE ACTUALLY DOING OUR JOB.
THE OTHER PANELISTS TODAY WILL TALK ABOUT WHERE WE CAN IMPROVE WHAT WE'RE DOING TO REDUCE THAT.
BUT SPAM CLICK THROUGH RATES HAVE BEEN GOING DOWN.
YES, SOME PEOPLE STILL DO CLICK ON THEM.
BUT COMPARED TO A DECADE AGO, THE PERCENTAGE OF THE POPULATION THAT ACTUALLY FOLLOWS SPAM IS DECREASING.
IF WE CAN CONTINUE TO DECREASE THAT, I THINK THAT MOBILE WILL CONTINUE TO BE IN MUCH BETTER SHAPE.
>> YOU THINK THAT'S SPECIFIC TO U.S. CONSUMERS?
OR IS THAT FOR THOSE OF YOU WHO ARE LOOKING MORE GLOBALLY, ARE YOU SEEING A DECLINE GLOBALLY AS WELL?
>> IF I MAY, I WOULD ECHO PATRICK'S POINT THAT MOBILE MALWARE TODAY IS NOT A TECHNICAL ISSUE.
IT'S SOCIAL ENGINEERING.
MOST OF THE DRIVE IS BECAUSE PEOPLE WANT SOMETHING FOR FREE.
IF THEY CAN FIND A GAME AND GET IT FOR FREE OR SLIGHTLY DODGY LINK RATHER THAN PAYING 1.99 IN PLAY STORE THEY TRY AND SAVE THE TWO BUCKS AND NOT REALIZE WHAT THEY'RE LOSING.
I THINK THAT'S THE SAME IN EVERY TERRITORY.

PEOPLE ALWAYS LOOK FOR SOMETHING
THAT'S FREE AND LOSE MONEY THAT
WAY.
>> I THINK WE NEED TO
DIFFERENTIATE A LITTLE BETWEEN
WHAT WE'RE TALKING ABOUT BECAUSE
WE'RE SAYING THAT A LOT OF THIS
IS BASED ON PHISHING, SOCIAL
ENGINEERING BUT THAT'S THE
ACCESS IN TO THE DEVICE.
ONCE IT GETS ON THE DEVICE THERE
ARE TECHNICAL RISKS THAT ARE
PRESENT INSIDE THE ANDROID iOS,
WINDOWS, DEVICES, THAT'S THE
JAIL BREAKS.
THE WITHOUT THAT THE ONLY DATA
THEY CAN ABUSE ARE THINGS LIKE
SENDING TOLL FRAUD, YOU KNOW,
BILL SHOCK, HOWEVER YOU GUYS
PHRASED IT, AS WELL AS
COLLECTING DATA THAT'S AVAILABLE
TO EVERY APPLICATION, BUT IF
THEY WANT YOUR BANKING
CREDENTIALS OR WANT YOUR TWITTER
CREDENTIALS OR SOCIAL MEDIA
CREDENTIALS OR OTHER ACCESS THEY
NEED THE BREAK OUT OF YOUR SAND
BOX AND THAT'S A TECHNICAL
ATTACK BASED ON TECHNICAL WEAK
NOSE A DEVICE IT'S INSTALLED
UPON.
THERE ARE CERTAIN MANUFACTURERS
THAT ARE BETTER AT HANDLING THAT
RISK AND CERTAIN THAT ARE WORSE.
THAT CREATES A REAL DIFFERENCE
FOR CONSUMERS.
>> TOTALLY AGREE BUT I WANT TO
AGAIN DIFFERENTIATE THAT IF THE
USER HAS TO CLICK 17 TIMES, I
REALLY WANT THE DOWNLOAD THIS,
YES, OKAY, OKAY, OKAY, JAIL
BREAK IT IS PHONE, IT REALLY IS
A SOCIAL ENGINEERING ISSUE.
YES, THE USER SAID YES.
SO AFTER A MUCH MORE DANGEROUS
ATTACK WOULD BE IF THE USER SAID

NOTHING.
WE'RE IN AGREEMENT YES, THERE
ARE ABSOLUTELY PROBLEMS WITH ALL
OF THE PLATFORMS, WITH ALL OF
THE PIECES OF TECHNOLOGY,
SOFTWARE HAS BUGS.
BUT WHAT I'M SAYING IS VECTOR IN
SEEMS TO BE PRIMARILY REQUIRING
THE USER TO DO SOMETHING.
>> I'LL ADD ONE THING.
A LOT OF LIKE FOLK ADVICE PEOPLE
GIVE ABOUT NOT INSTALLING
MALICIOUS APPLICATIONS ON
ANDROID THAT'S NOT CORRECT.
A LOT CENTERS ON PERMISSION AND
WHETHER THE PERMISSION ON GIVEN
APPLICATION ASKS FOR ARE ASKING
FOR TOO MUCH.
BUT WHEN WE LOOK AT WHAT JAIL
BREAKS REQUIRE IN TERMS OF
PERMISSION TO BE ABLE TO RUN,
IT'S NOTHING.
SO THE KINDS OF THINGS YOU
THATTED TO CLICK THROUGH ARE
MINIMAL.
THE APP WILL ASK FOR VERY LITTLE
BUT PERMISSION THAT IT CAN GAIN
BY ITSELF THROUGH AN ATTACK IS
ACTUALLY VERY LARGE.
SO THAT MISMATCH MAKES IT MORE
OF A RISK BECAUSE CONSUMERS
AREN'T GOING TO BE ABLE TO TELL.
>> MY QUESTION CARDS ARE
BUILDING UP TO A LARGE STACK.
SO FIRST OF ALL, I'M SUPPOSED TO
REMIND EVERYONE IF YOU HAVE ASKS
FOR PANELISTS, WRITE THEM ON A
CARD, HOLD THEM UP FOR THOSE OF
YOU WHO MAY HAVE COME LATE.
AND I DO WANT TO GET TO A COUPLE
QUESTIONS.
ONE IS VIA TWITTER, WHAT CAN
CELLULAR PROVIDERS DO TO DETECT
MOBILE DEVICES EFFECTED WITH
MALWARE AND PRE-RENT DELIVERY OF
MALICIOUS TRAFFIC.

THAT SEEMS LIKE A GARETH
QUESTION.
I THINK IT'S FROM THE CFTC.
>> OPERATORS FROM WHERE THEY SIT
CAN DO A LOT TO FIND OUT WHICH
DEVICES ARE INFECTED.
ONE OF THE THINGS WE DO BY
LOOKING AT THE TRAFFIC THAT
ACTUALLY FLOWING THROUGH THAT
NETWORK, WE CAN IDENTIFY WHICH
DEVICES ARE COMPROMISED AND WHAT
THEY'RE COMPROMISED WITH.
AND OUR STATS END UP BEING
SOMEWHERE BETWEEN OMAR AND
PATRICK'S, CLOSER TOWARD
PATRICK'S END THAN OMAR.
WE DON'T SEE A LOT OF INFECTIONS
IN NETWORKS TODAY.
TO KEEP FROM THE AN OPERATE TO,
THE REASON THEY'RE LOOKING AT
THIS IS NOT NECESSARY TO TRY TO
STOP PEOPLE FROM BECOMING
INFECTED.
SO MANY DIFFERENT WAYS YOU CAN
INFECT A PHONE BUT AN OPERATOR
CAN'T ACTUALLY KEEP PEOPLE SAFE
ALL THE TIME.
BUT THE CONCERN FOR THEM IS THE
PUBLIC ARE AWARE OF MOBILE
THREATS.
TALKING TO MY MOTHER THE OTHER
DAY, GOT AN ANDROID SMARTPHONE,
SHE WAS NERVOUS ABOUT WHAT SHE
DOWNLOADED IN CASE SHE GOT A
VIRUS.
WHAT HAPPENS IS EVERY TIME A
CONSUMER FINDS THAT THEY HAVE
GOT A CHARGE ON THEIR BILL
THEY'RE NOT SURE ABOUT OR CREDIT
DISAPPEARED OR BATTERY RUN DOWN,
THE FIRST THING THEY DO IS PHONE
THE OPERATOR, MUST BE A VIRUS I
READ ABOUT THEM.
AND THAT CALL COSTS THE OPERATOR
10 TO 15 DOLLARS EVERY SINGLE
TIME.

SO ACTUAL FEAR OF MOBILE MALWARE, FEAR OF INFECTION CAN BE MUCH MORE COSTLY PROBLEM FOR OPERATORS THAN ACTUAL NUMBER OF INCIDENTS HAPPENING TODAY.
>> OMAR, ARE THERE CERTAIN GROUPS OR POPULATIONS WITHIN THE U.S. THAT ARE MORE VULNERABLE THAN OTHERS IN I MEAN I THINK YOU IDENTIFIED TEENS AS ONE OF THE REALLY VULNERABLE POPULATIONS BECAUSE OF THEIR BEHAVIOR.
ARE THERE OTHERS YOU'VE IDENTIFIED THAT PARTICULARLY NEED TO KNOW ABOUT THIS?
>> I MEAN I THINK OTHER THAN A SPECIFICALLY IDENTIFYING TEENS OR KIDS WHO ARE MORE LIKELY AS DAN SAID OR AS GARETH SAID LOOKING FOR WAYS AROUND GETTING GAMES AND GETTING OTHER TYPES OF APPLICATIONS AND DOWNLOADING FREE TOOLS, FREE APPLICATIONS, FOR US THAT'S BEHAVIORAL.
WE HAVEN'T NECESSARILY SEGMENTED FROM PERSONAL INFORMATION DOWN BECAUSE WE DON'T COLLECT THAT LEVEL OF PERSONAL INFORMATION DOWN TO SPECIFIC DEMOGRAPHICS THAT ARE MORE AT RISK VERSUS HIGHER AT RISK.
SO WE HAVEN'T GOTTEN DOWN TO THAT POINT.
I THINK IN GENERAL, YOU WOULD ASSUME, WOULD YOU MAKE THE ASSUMPTION BASED ON OUR OWN PANELS OR FOCUS GROUPS THAT WE HAVE DONE, IT TENDS TO BE IN ENVIRONMENTS LESS TECH SAVVY, YOU KNOW, THAT ARE LESS NECESSARILY LESS AWARE OF WHAT THEY'RE DOING, WHAT A SPECIFIC CLICK OR SPECIFIC PERMISSION SET IS THAT YOU'RE GIVING ACCESS TO ON A DEVICE.

BEYOND THAT,
[PLEASE STAND BY]
[PLEASE STAND BY]
THERE HAVE BEEN INCIDENCE
REPORTED IN THE MEDIA, LAST
THREE MONTHS THAT TOOK ADVANTAGE
OF SEVERAL LEGITIMATE
APPLICATIONS ON THE APP STORE
THROUGH THAT METHOD.
>> OKAY.
GARETH, WHERE DO YOU SEE THINGS
HEADED?
>> PROBABLY THREE AREAS THAT
WE'RE TRACKING.
THE FIRST BACK TO A POINT FROM
THE OPENING COMMENTS BY STATE,
ACTUALLY THESDKs USED TO BUILD
APPS, LOOKING AT HOW ORGANIZED
GROUPS CAN PUT TOGETHER
NEW SDKs, MAKE THEM AVAILABLE TO
DEVELOPERS WHO ALREADY HAVE
SOMETHING WITH A BACKDOOR
INCLUDED IN A RANGE OF
APPLICATIONS.
PENNED TIME LOOKING AT THE
MACHINE TO MACHINE ENVIRONMENT
THAT'S OUT THERE BECAUSE WE COME
FROM A NETWORK CENTRIC.
THERE ARE DEVICES THAT RELY ON
SIM CARDS, CELLULAR DATA TO
COMMUNICATE BETWEEN EACH OTHER.
RATHER THAN CONSUMER OR
INDIVIDUAL BEING ATTACKED, IS
LOOKING AT THE SECURITY OF THE
SERVICES, WITS HOME AUTOMATION,
FLOOD CONTROL, ET CETERA, THAT
COULD BE COMPROMISED.
I THINK THE NEW AREAS ACTUALLY
THE NEW SERVICES THAT THE
OPERATORS DESPERATELY TRYING TO
LAUNCH, YOU MAY HAVE HEARD
OF RCS, RICH COMMUNICATION
SERVICES, WHICH IS REALLY THE
CELLULAR INDUSTRY'S APPROACH TO
DEALING WHAT'S HAPPENING WITH
OTHER OVER THE TOP MESSAGING

SERVICES.
NOW, THOSE OFFER HUGE GREAT
OPPORTUNITIES IN TERMS OF WAYS
IN WHICH DEVICES CAN INTERACT WE
HAVE OTHER, TALK TO EACH OTHER,
FIND OUT WHICH DEVICES ARE
POTENTIALLY VULNERABLE FOR
ATTACKS IN CARRYING NEW ATTACKS,
THAT'S NARROWLY FOCUSED WITH APT
RATERS AT THE MOMENT, OPERATORS
AT THE MOMENT.
>> I AGREE WITH COLLEAGUES, ALL
EMERGING THREAT FACTORS.
I AGREE THAT MOBILE BROWSERS
PROBABLY EMERGING OPPORTUNITY
ALTHOUGH MUCH MORE COMPLEX.
I THINK WHAT'S GOING TO END UP
HAPPENING ESPECIALLY AS WE HEAD
IN TO THE NEXT GENERATION OF
MOBILE BROWSERS AS MORE AND MORE
DEVICE LEVEL APIs EXPOSED WITHIN
THE BROWSER FOR BROWSER-BASED
APPLICATIONS YOU'LL SEE QUITE A
BIT MORE ACTIVITY FROM A
SOPHISTICATION STANDPOINT
BECAUSE I THINK AS WE HEAD IN TO
THE FUTURE ENVIRONMENT TODAY,
LARGELY I THINK EVERYONE AGREES
ON THIS PANEL THAT IT IS REALLY
APP BASED DISTRIBUTION BECAUSE
OF HOW EASY HAS TO DEPLOY APPS,
BECAUSE OF THE NEWSPAPER OF APIs
THAT APPS HAVE ACCESS TO, WHERE
THE VULNERABILITY IS, WHERE THE
THREAT SECTOR IS.
AS WE HEAD FORWARD, WHERE YOU
HAVE, WHERE APPLICATIONS AND
FUNCTIONALITY STARTS TO MIGRATE
BACK TOWARDS THE BROWSERS,
BECOME MORE AND MORE POWERFUL ON
MOBILE DEVICE YOU'LL SEE MORE
AND MORE APIs EXPOSED TO THAT
DIRECTION, YOU'LL SEE THIS
NATIVE, SORRY, THIS HYBRID
ENVIRONMENT DEVELOP WHERE YOU
HAVE NATIVE WRAPPERS, CODE

EMBEDDED SO IT CHANGES THE LANDSCAPE.
DOESN'T MEAN EXACTLY HOW IT WILL EMERGE BUT THAT EVOLUTION WILL DRIVE NEW LEVEL ATTENTION FROM HACKERS AND CREATE BEING SPOEGS SURE.
>> YOU THINK A SHIFT BACK TO BROWSERS IN HOW PEOPLE USE MOBILE DEVICES AND THAT'S GOING TO MEAN THAT'S WHERE THE MALWARE WILL SHIFT AS WELL?
>> IT'S ALREADY HAPPENING, RIGHT?
ALREADY HAPPENING IN TERMS OF MORE AND MORE FUNCTIONALITY GOING BACK TOWARDS THE BROWSER.
DOESN'T MEAN NATIVE APPLICATIONS ARE GOING AWAY ANY TIME SOON, THEY'RE NOT.
BUT THERE'S MORE AND MORE FUNCTIONALITY EMBEDDED WITHIN THE BROWSER BASED FUNCTIONAL BEING, SUPPOSED TO USERS.
EXPOSED TO USERS, WHETHER IT'S PHISHING OR OTHER INCURSIONS WILL INCREASE IN FREQUENCY AS WELL.
>> OKAY.
OMAR, GARETH, DAN, PATRICK, THANK YOU SO MUCH FOR BEING HERE TODAY.
I'M SURE PEOPLE WOULD APPRECIATE IF IT YOU STUCK AROUND A LITTLE DURING THE BREAK IN CASE THEY CAN'T TO HARASS YOU WITH QUESTIONS.
FOR EVERYONE ELSE, BE BACK AT 10:55 FOR OUR NEXT PANEL.
THANK YOU.
[APPLAUSE]