FTC Fall Technology Series: Ransomware
September 7, 2016
Segment 1
Transcript

>> MY NAME IS BEN ROSSEN BEFORE

WE GET STARTED WITH THE PROGRAM

I NEED TO GO OVER A FEW

ADMINISTRATED DETAILS I'M

OBLIGATED TO SHARE WITH YOU.

IF YOU COULD, PLEASE SILENCE

MOBILE PHONES AND DEVICES.

IF YOU NEED TO USE THEM DURING

THE WORKSHOP BE RESPECTFUL OF

SPEAKERS AND FELLOW AUDIENCE

MEMBERS.

IF YOU LEAVE CONSTITUTION

CENTER, THIS BUILDING, DURING

ANY REASON FOR -- DURING THE

WORKSHOP FOR ANY REASON YOU WILL

HAVE TO GO THROUGH SECURITY

AGAIN.

THE REST ROOMS DROWN THE HALL

OUT OF THE AUDITORIUM.

THE PLAZA EAST CAFETERIA IS

INSIDE OF THE BUILDING.

IT'S ONLY OPEN UNTIL 3:00 P.M.

MOST OF YOU RECEIVED A LAN.

YARDSECURITY BADGE.

WE REUSE THESE.

PLEASE RETURN THEM TO EVENT

STAFF.

IF A EMERGENCY OCCURS REQUIRING

US TO LEAVE THE ROOM BUT REMAIN

IN THE BUILDING FOLLOW THE

INSTRUCTIONS OVER THE BUILDING

PA SYSTEM.

IFFY EVACUATION IS REQUIRED AN

ALARM WILL SOUND.

EVERYONE SHOULD LEAVE THE

BUILDING IN AN ORDERLY MANNER

THROUGH THE MAIN SEVENTH STREET

EXITS.

TURN LEFT ACROSS E STREET TO THE

EMERGENCY ASSEMBLY AREA WHERE WE

ASK YOU TO REMAIN

UNTILINSTRUCTED TO RETURN TO THE

BUILDING.

ADVICE THIS EVENT MAYBE

PHOTOGRAPHED.

IT'S BEING WEB CASTD AND

RECORDED.

BY PARTICIPATING IN THE EVENT

YOU AGREE YOUR IMAGE AND WHAT

YOU SAY OR SUBMIT MAYBE POSTED

INDEFINITELY.

WE ARE HAPPY TO WELCOME EVERYONE

SKRAOE A WEB CAST.

WE WILL MAKE ALL MATERIALS

AVAILABLE ON-LINE TO MAKE A

LASTING RECORD.

FOR THOSE ON TWITTER FTC STAFF

WILL LIVE TWEET TODAY'S WORK

SHOP USING THE #RANSOMWAREFTC.

WORK SHOP STAFF WILL COLLECT

QUESTIONS.

BRING THEM TO THE MODERATORS.

RAISE YOUR HAND AND WE WILL

COLLECT THOSE UP.

AS ONE OF THE REMINDERS THE

PUBLIC COMMENT PERIOD WILL BE

OPEN THRUG OCTOBER 7th, 2016.

I URG YOU IF YOU'RE TAKING TIME

TO BE PART OF THE EVENT SUBMIT

COMMENTS AT OUR WEBSITE FTC GOV.

LASTLY THANK YOU TO OUR

PANELISTS TAKING PART TODAY

WE'RE GRATEFUL OF YOUR TIME AND

CAREFUL CONSIDERATION OF THE

ISSUES.

WE'RE EXCITED TO HEAR YOUR

THOUGHTS.

ASIDE FROM FOLKS YOU SEE TODAY

ON STAGE THIS PROGRAM WOULD NOT

BE POSSIBLE BY THE GREAT WORK OF

FOLKS AT THE COMMISSION.

ALL OF OUR PARA LEGAL SUPPORT

ALSO.

WITHOUT FURTHER A DO I'M PLEASED

TO WELCOME OUR CHAIR WOMAN

EDYTHE RAMIREZ.

[APPLAUSE]

>> THANK YOU, BEN.

GOOD AFTERNOON, EVERYONE.

WELCOME TO AS BEN MENTIONED THE

FIRST OF OUR FALL TECHNOLOGY

SERIES.

FROM THE EARLIEST DAYS OF THE

INTERNET CRIMINALS HAVE USED AN

ARRAY OF TACTICS TO TRICK

CONSUMERS TO DOWNLOADING

MALWARE, SPYBARE AND OTHER

UNWANTED SOFTWARE TO COMPUTERS

AND DEVICES.

THIS SOFTWARE MAKES OUR

COMPUTERS VULNERABLE, ALLOW

SPHOPB TORING FOR SCAMMERS, AND

A PATHWAY TO STEAL PERSONAL

INFORMATION WHICH THEY CAN USE

TO PERPETRATE FRAUD.

IN RECENT YEARS CRIMINALS HAVE

FOUND A NEW BUSINESS MODEL IN

THE FORM OF RANSOMWARE.

THIS MALWARE INFILTRATES A

COMPUTER SYSTEM AND USES TOOLS

LIKEN DESCRIPTION TO USE

VALUABLE DATA HOSTAGE IN

EXCHANGE FOR A RANSOM.

CRIMINALS HAVE CREATED A NEW
MARKET FOR PERSONAL INFORMATION,
MAKING RANSOMWARE MORE
PROFITABLE THAN OTHER SCAMS.
IN FACT RECENT REPORTS DESCRIBE
RANSOMWARE AS THE MOST
PROFITABLE MALWARE SCAM IN
HISTORY.
NOBODY IS IMMUNE.
INDIVIDUAL CONCERNS, TKPOFT
AGENCIES AND ENTITIES OF ALL
TYPES AND SIZES HAVE BEEN
TARGETS.
THE ATTACK ON HOLLYWOOD
PRESBYTERIAN MEDICAL CENTER
EARLIER THIS YEAR IN CALIFORNIA.
THE FIRST ON A STRING OF
ATTACKS, HIGHLIGHTS THE
CHALLENGES OF RANSOMWARE.
THEY TOOK OUT THE ENTIRE NETWORK
OF THE HOSPITAL FOR MORE THAN A
WEEK.
LEAVING STAFF WITHOUT E-MAIL OR

CRITICAL PATIENT DATA. IT
CRIPPLED THE EMERGENCY ROOM AND
OTHER COMPUTER SYSTEMS FOR
PATIENT.
ULTIMATELY THE HOSPITAL PAID A
RANSOM OF 40BIT COINS OR $17,000
TO RESTORE IT'S OPERATIONS.
ANOTHER ATTACK IN MARCH DISABLED
MEDSTAR HEALTH COMPUTER SYSTEMS
DENYING ACCESS TO E-MAIL AND
PATIENT RECORDS FOR TEN
HOSPITALS IN THE WASHINGTON DC
REGION FOR NEARLY TWO WEEKS.
IT'S NOT SURPRISING THAT
RANSOMWARE IS AMONG THE MOST
TROUBLE CYBER THREATS.
TODAY WHAT I WOULD LIKE TO DO IS
HIGHLIGHT SOME KEY CHALLENGES
ASSOCIATED WITH RANSOMWARE AND
THE IMPORTANT ROLL THAT I SEE
BUSINESSES AND THE FEDERAL TRADE
COMMISSION PLAY IN COMBATING
THIS GROWING THREAT.

THE RANSOM.

SOME WARE THREAT SIN CREASINGLY

MORE PERNICIOUS.

FIRST THE STATE OF RANSOMWARE

INCIDENTS ARE ESCALATING AT AN

ALARMING RATE.

THEY HAVE QUADRUPLED IN THE LAST

YEAR ALONE AVERAGE 4000 A DAY.

THE FINANCIAL MOTIVATION FOR

RANSOMWARE ATTACKS SUGGESTS THE

THREAT IS UNLIKELY TO GO AWAY

ANYTIME SOON.

ACCORDING TO DATA FROM SCIENCE

INC. TYPICAL PAYMENTS ARE $500

TO A THOUSAND DOLLARS.

SOME CRIMINALS HAVE DEMANDED AS

MUCH AS $30,000.

THE PERM TRAITORS OF RANSOMWARE

ATTACKS ARE USING A WIDE RANGE

OF TACTICS TO LURE THEIR TARGETS

TO DOWNLOADING MALICIOUS

SOFTWARE.

BEFORE IT WAS SPAM E-MAIL USED

TO DELIVER RAM SO MANYWARE.

AS SPAM FILTERS HAVE GOTTEN

BETTER SOME HAVE TURNED TO SPEAR

FISHING TARGETING SPECIFIC

INDIVIDUALS OR ORGANIZATIONS.

93% OF FISHING MALES HAVE SOME

VARIANT OF RANSOMWARE.

OTHERS AVOID E-MAIL ALL TOGETHER

PLANTING MALICIOUS CODE ON

SEEMING LESS EXPLOSIVE WEB SITES

AND PATCHES ON SERVERS.

ONE VERSION SAM SAM EXPLOITS A

WEB SERVING APPLICATION FOUND IN

OVER 3.2 MILLION MACHINES USED

MAINLY BY SCHOOLS, LOCAL

GOVERNMENTS AND AVIATION

COMPANIES.

AS SOME OF THE PANELISTS TO DAY

WILL EXPLAIN CYBER CRIMINALS

DEVICE NEW AND CREATIVE METHODS

FOR SPREADING THE MAL WARE.

THE HARM IS ALSO RISING.

ATTACKS TARGETING CONSUMERS

CAPITALIZE ON THE FACT THAT
VICTIMS ARE LIKELY TO PAY TO
PREVENT LOSING IMPORTANT
DOCUMENTS OR REPLACE PERSONAL
ITEMS LIKE FAMILY PHOTOS.
SOME NEW FORMS TARGET CONSUMER'S
MOBILE DEVICES.
RENDERING THEM COMPLETELY
INOPERABLE.
ATTACKS TARGETING BUSINESS CAN
IMPOSE SIGNIFICANT COSTS.
EVEN BEYOND THE MONETARY LOSSES
ATTACK ON BUSINESSES CAN HAVE
DEVASTATING AFFECTS ON
CONSUMERS.
FOR EXAMPLE RAP SO MANY WARE
ATTACKERS MAY STEAL EXTREMELY
SENSITIVE CONSUMER INFORMATION.
SUCH AS MEDICAL DATA, FINANCIAL
ACCOUNT NUMBERS, AND THE CONTENT
OF PRIVATE COMMUNICATIONS THAT
CAN BE SOLD ON THE DARK WEB.
SHUTTING DOWN A COMPANY'S

ABILITY TO WORK CAN HURT
CONSUMERS SUCH AS ACCESS TO
MEDICAL RECORDS IN AN EMERGENCY.
AS WELL AS THE INCREASE AND
SOPHISTICATION AH TACKS AT THE
FTC WE'RE EAGER TO UNDERSTAND
THE GROWING THREAT.
AS AN AGENCY ADDRESSING MALWARE
AND THE HARM, INCLUDING
CHALLENGES TO CONSUMER DATA, THE
FTC PLAYS A UNIQUE ROLL.
FOR NEARLY A DECADE WE WORKED
WITH OTHER AGENCIES AND PROVIDED
GUIDANCE TO CONSUMERS AND
BUSINESS ONS HOW TO BEST PROTECT
THEIR CONSUMERS AND NETWORKS.
IN 2014 THE FTC ALONG WITH THE
FBI AND OTHER AGENCIES ISSUE
WARNINGS ABOUT CRYPTO LOCKER.
A EARLY FORM OF CRYPTO
RANSOMWARE.
THESE TIPS ARE NO LESS RELEVANT
TODAY.

THE FTCs PRIVACY AND DATA
SECURITY LABS EXPRESS SECURITY
WHICH CAN PREVENT RANSOMWARE
ATTACKS.
WE HAVE BROUGHT APPROXIMATELY 60
ENFORCEMENT ACTIONS AGAINST
COMPANIES THAT HAVE FAILED TO
REASONABLY SECURE CONSUMER DATA
ON NETWORKS.
WE AIM FOR COMPANIES TO MAKE
TRUTHFUL REPRESENTATION ABOUT
THEIR SECURITY PRACTICES AND
PROVIDE REASONABLE INFORMATION
FOR CONSUMERS.
ONE COMPONENT IS THAT COMPANIES
HAVE PROCEDURES IN PLACE TO
ADDRESS VULNERABILITIES AS THEY
ARISE INCLUDING MALICIOUS
SOFTWARE.
A FAILURE TO PATCH
VULNERABILITIES MAY VIOLATE THE
FTC ACT.
IN A RECENT CASE AGAINST DEVICE

MANUFACTURE ASIS WE ALLEGE THE
COMPANY'S PERVASIVE SECURITY
BUGS LEFT THE COMPANY OPEN TO
MALWARE AND ATTACKERS DID THIS
TO RECONFIGURE SETTINGS AND TOOK
CONTROL OF CONSUMERS WEB
ACTIVITY.
WE ALLEGED THE COMPANY DIDN'T
ADDRESS THE SECURITY
VULNERABILITIES IN A TIMELY
MANNER AND FAILED TO INFORMATION
CONSUMERS ABOUT THE VULNERABLE
ROUTERS.
AGAINST WYNDAM WORLDWIDE HACKERS
INFILTRATED.
THEY PLACED MEMORY SCRAPING
MALWARE ON THE FRANCHISE
SERVERS.
WE ALLEGE THE HACKERS THEN
EXPLOITED THE VULNERABILITIES TO
STEAL DATA FROM DOZEN OF
FRANCHISES.
AS THIS IS CLEAR BUSINESSES PLAY

A CRITICAL ROLL TO ADEQUATELY

PROTECT CONSUMER INFORMATION.

PARTICULARLY AS SECURITY THAETS

ESCALATE, LIKE RANSOMWARE.

AS WE LEARN MORE ABOUT THE

IMPACT AND SCOPE OF THE RANSOM

WARE ATTACKS WE FIND OURSELVES

FACING A NUMBER OF QUESTIONS.

FOR EXAMPLE ARE THE STEPS

CONSUMERS AND BUSINESSES SHOULD

BE TAKING TO REDUCE THE RISK OF

RANSOMWARE OR DECREASE THE

IMPACT?

WHAT CAN BE LEARNED FROM

CRIMINAL LAW ENFORCEMENT EFFORTS

TO COMBAT THE ATTACKS.

THESE ARE JUST A FEW OF THE

QUESTIONS WE WILL ATTEMPT TO

ANSWER DURING TODAY'S WORK SHOP.

MY HOPE THIS S. THIS DISCUSSION

WILL PROVIDE VALUABLE INSIGHT TO

THE CHALLENGES OF THE RANSOMWARE

THREAT AND PROVIDE PRACTICAL

ADVICE ON MEETING THE

CHALLENGES.

I HOPE BY THE TIME YOU LEAVE

HERE THIS AFTERNOON YOU WILL

HAVE A BETTER UNDERSTAND OF THE

THREATS POSED BY RANSOMWARE.

THE VECTORS USED BY A STACKERS

AND THE TOOLS THAT ARE USED TO

SAFE GUARD DATA. IN THE MONTHS

AHEAD I HOPE WILL YOU CONTINUE

TO WORK WITH US TO HELP ADDRESS

THIS VERY CHALLENGING ISH AO +*UZ

AOU.

BEFORE WE TURN TO THE FIRST

PANEL I WANT TO TAKE THIS

OPPORTUNITY TO THANK FTC STAFF

FROM OUR DIVISION OF PRIVATE SEE

AND IDENTITY PROTECTION,

MARKETING PRACTICES AND

RESEARCH/INVESTIGATION FOR

ORGANIZING THE WORK SHOP TODAY.

I WOULD LIKE TO THANK BILL, MAX,

STEVE AND JOE AS WELL AS OUR

SPEAKERS WHO HAVE GATHERED HERE

TO SHARE THEIR VERY VALUABLE

INSIGHTS.

THANK YOU, VERY MUCH.

[APPLAUSE]

;;;;Panel 1

>> THANK YOU, SO MUCH, EDITH

RAMIREZ.

IT'S MY PLEASURE TO TURN IT TO

OUR FIRST PANEL OF THE DAY: OVER

VIEW OF THE RANSOMWARE THREAT.

OUR MODERATOR STEVE WERNIKOFF.

>> THANKS TO -- THANKS TO CHAIR

WOMAN RAMIREZ FOR THE GREAT KICK

OFF REMARKS.

WELCOME TO THE FIRST PANEL.

MY NAME IS STEVE WERNIKOFF I'M

THE ENFORCEMENT OFFER FROM

OFFICE OF TECHNOLOGY RESEARCH

AND INVESTIGATION.

WE'RE LOOKING AT RANSOMWARE

THREAT.

WE HAVE FOUR EXPERTS JOINING US.

I AM DOING A SHORT INTRODUCTION.

IN THE INTEREST OF TIME I WON'T

READ THEIR FULL BIOS.

I ASK YOU TO TAKE A LOOK AT

THEIR PIES.

WE HAVE A VERY ACCOMPLISHED

GROUP WITH US THIS MORNING.

AT THE FAR END CRAIG WILLIAMS.

JOE OPACKI.

LANCE JAMES.

GEORGIA WEIDMAN.

OUR EXPERTS WILL GIVE FOUR SHORT

PRESENTATIONS ON DIFFERENT

ASPECTS OF THE RANSOMWARE ISSUE.

OUR GOAL IS TO PROVIDE A HIGH

LEVEL OVER VIEW OF THE

RANSOMWARE THREAT AND SET THE

TABLE FOR THE ADDITIONAL PANELS

IN THE WORK SHOP TODAY.

IF TIME PERMITS WE WILL ANSWER

QUESTIONS.

THERE ARE COMMENT CARDS IN THE
FRONT FRONT AND OTHER FTC
PERSONNEL AROUND WITH COMMENT
CARDS.
PLEASE WRITE YOUR QUESTIONS ON
THE CARDS.
THEY WILL GET FILTERED TO THE
FRONT HERE.
ON THE WEB CAST, IF YOU HAVE ANY
QUESTIONS AND WANT TO TKWAOET
THE QUESTIONS WE WILL OF COURSE
TRY TO GET TO THOSE TOO.
SO, TO START THINGS OFF WE HAVE
CRAIG WILLIAMS.
CRAIG WILL GIVE AN OVER VIEW OF
THE HISTORY OF RANSOMWARE AND
DISCUSS HOW IT AFFECTS CONSUMERS
AND BUSINESSES.
YOU'RE WELCOME TO SIT OR STAND,
WHATEVER.
>> I WILL STAND.
>> SO, MY NAME IS CRAIG
WILLIAMS.

I'M FROM AN ORGANIZATION AT

CISCO KNOWN AS TALOS.

IT'S THE SECURITY AND RESEARCH

OF CISCO.

THE REASON I WANTED TO TALK TO

YOU TODAY IS THE PROBLEM OF

RANSOMWARE IS IT HAS THE HIGHEST

MONETARY VALUE FOR ADVERSARIES.

WE HAVE MOVED FROM AN ATTACKER

MAKING A COUPLE OF DOLLARS TO

USER, NOW THEY'RE MAKING A

COUPLE OF HUNDRED PERUSERS AND

TENS OF THOUSANDS FOR

COMPROMISING BUSINESS.

IT HAS PUT IT ON A SCALE WE

HAVEN'T SEEN BEFORE.

IT'S ATTRACTIVE FOR OUR

ADVERSARIES.

GIVEN THAT MONEY AND INCOME THEY

CAN HIRE PROFESSIONAL

DEVELOPMENT TEAMS ACROSS THE

WORLD TO EVOLVE AND DEPLOY

MALWARE AT AN AMAZING RATE.

WE HAVEN'T SEEN ANYTHING LIKE

IT.

IT'S REALLY JUST A PROCESS THAT

IS GROWING FASTER AND FASTER

WITH FUNDING GETTING BIGGER.

TO PUT THIS IN PERSPECTIVE IF

YOU DON'T KNOW WHAT RANSOMWARE

IS IT'S NOT NEW.

THE MOST COMMON IS CRYPTO WALL

3.

WHAT IS SO INSIDIOUS IS OVER A

NUMBER OF YEARS IT CONVINCED

PEOPLE THAT RANSOMWARE WAS

TRUSTWORTHY.

WE KNOW, ON THE STAGE, IT'S NOT.

A USER OR HOME OFFICE.

MY FRIEND GOT INFECTED WITH

RANSOMWARE THEY PAID $500 AND

GOT FILES BACK.

WE SEE THIS IN THE NEWS AND

MEDIA, TIME AND TIME AGAIN.

THE BENEVOLENT BAD GUYS GIVE THE

FILES BACK.

THAT'S NOT ALWAYS THE CASE.

SOMETHING CAN GO WRONG OR THE

BAD GUY DECIDES I WANT MORE

MONEY.

WE WILL TALK ABOUT SAM SAM IN A

MOMENT.

THE SAM SAM ACTORS WE REGULARLY

SAW THEM WANT MORE MONEY.

RANSOM -- DESPITE THE IMAGE THAT

THEY CAN.

IT'S TO THE EXTENT SOMEONE

HITTING THE BIG EXCHANGE ON A

BAD GUY AND THE BENEVOLENT BAD

GUYS GAVE THE FILES BACK.

IF I COME TO YOUR APARTMENT AND

ROB THE APARTMENT AND PUT A

LETTER ON THE DOOR SAYING I HAVE

TAKEN EVERYTHING YOU OWN.

IF YOU SEND ME $500 TO A PO BOX

I PROMISE TO SEND YOU A KEY TO A

STORAGE UNIT WHERE IT'S ALL

STORED.

ABSURD.

NOBODY WOULD FALL FOR IT THAT'S
THE REALITY OF RANSOMWARE AND
PEOPLE TRUST THEM WITH THE
HISTORY OF SOME FILES GIVEN
BACK.
THE FIRST PIECE OF RANSOMWARE
WAS WRITTEN IN 1915.
IT WAS A TROJAN AND PHYSICALLY
ASKED PEOPLE TO SEND MONEY
THROUGH THE U.S. MAIL.
ANY PROBLEM WITH THAT APPROACH.
>> IT'S EASY TO TRACE WITH A
PHYSICAL ADDRESS.
FOR ABOUT TEN YEARS IT TK-RPBT
EVOLVE.
RANSOMWARE WAS STAGNANT.
SOMEONE HAD THE IDEA BUT IT
WASN'T USED.
THEY ASKED FOR RANSOM OF $189
DISTRIBUTED BY A CASSETTE.
IT WASN'T A BIG DEAL AND THE
AUTHOR'S HISTORY IS INTERESTING.
WE SAW THIS EVOLVE INTO THINGS

LIKE GPC CODER.

THAT EVOLVED A BIT.

THIS IS ONE OF MY FAVORITES

REVETON.

DEPENDING WHERE YOU WERE

GEOGRAPHICALLY LOCATED IT WOULD

HAVE A DIFFERENT SCREEN.

IN THE U.S. IT WAS FBI.

IN EUROPE IT WAS INTERPOLL.

FBI INFECTS YOUR COMPUTERS AND

DEMAND A RANSOM.

IF YOU READ IT, IT WILL ACCUSE

YOU OF CRIMES.

IF YOU PAY THE FINE FOR THE

CRIMES IT'S OKAY.

IT'S BASIC MANIPULATION TO THE

USER.

AS SOON AS THE TOR PROJECT TOOK

OFF AND BY THECOIN IT WAS A

CHANGE FOR RANSOMWARE.

IT WAS A CYBER CRIME.

WHEN YOU HAVE BITCOIN YOU

EFFECTIVELY HAVE A SYSTEM THAT

CAN'T BETRAYED OR STOPPED.

THAT CAN BE PAID TO PEOPLE TO

WRITE MALWARE.

YOU HAVE A UNTRACEABLE SYSTEM OF

CURRENT SEE.

IMMEDIATELY THAT SOLVES THE

BIGGEST PROBLEM THAT THE TROJANS

HAD AND OTHER RANSOMWARE HAD.

BASICALLY IT TOOK OFF.

WE HAD CRYPTOWALL, CRYPTO

LOCKER, SAM SAM, CTB-LOCKER.

THERE HAVE BEEN VARYING DEGREES

OF SUCCESS.

I DON'T WANT TO BE A GLASS EMPTY

GUY.

SOME OF THESE ARE -- I BELIEVE

SHORTLY AFTER THIS FOR THE NEXT

VERSION A INDEPENDENT TEST WAS

RELEASED.

OVER A PERIOD OF 18 MONTHS THE

SECURITY KICKED OUT THE DESK

FROM THE BAD GUYS DESTROYING

THEIR MODEL.

WHEN YOU THINK OF THE MONEY IT

TAKES TO WRITE THE SOFTWARE WE

BROKE THAT IN AN INDUSTRY.

ABOUT A MONTH AGO THE AUTHORS

GAVE UP.

THEY POSTED A WEBSITE AND SAID

SORRY.

THIS ISN'T TO SAY IT'S AN EASILY

SOLVED ISSUE.

THERE IS RANSOMWARE THAT DOES IT

RIGHT AND WE'RE LOOKING FOR WAYS

TO COMBAT THOSE.

THE NEXT THING I WANT TO TALK

ABOUT IS RANSOMERS DEPLOYED.

WE HAVE SEEN THE SPAM

METHODOLOGY.

WE SEE HUNDREDS OF THOUSANDS OF

LOCKY EVERY DAY.

I WOULD EXAMINE THE NUMBERS YOU

THINK, WE SEE THEM OTHERWISE.

COMBINE THAT WITH AUTOMATION AND

IT GROWS ASTRONOMICALLY.

IF YOU'RE NOT FAMILIAR WITH

MAGVERTIZING IT'S THE NUMBER ONE

THREAT.

I HAVE PEOPLE SAY WE'RE SECURE.

THE MODEL DOESN'T WORK ANYMORE.

>> IF ADS ARE ON THE INTERNET

IT WILL NEVER WORK.

IT'S WORST NOW.

WE SEE CERTAIN WEB SITES

BLOCKING USE WERZ AD BLOCKERS

KNOWING THEY RUN AN INFECTIOUS

AD STREAM.

SEVERAL U.S. NEWS SITES.

BUSINESS SITES DO THIS.

THE WAY MALEVTISING WORKS YOU

HAVE AN AD SERVICE AND IT

REDIRECTS YOU.

99.8 PERCENT OF THE TIME IT'S

FINE AND LEGITIMATE AD.

YOU SEE IT.

THE BUSINESS AGAINST ONE

MILLIONTH OF A PENNY.

THE SMALL FRAC OF THE TIME,

THEY'RE REDIRECTED TO A

DIFFERENT SERVING, THAT TO A
MALICIOUS SERVICER AND THEN TO A
LANDING PAGE.
WE SEE THIS DAILY AT CISCO.
AS A SECURITY RESEARCHER OR AD
MIN. YOU SEE THIS, YOU SAY THE
INTRUSION PREVENTION SYSTEM SAID
I SAW THE NUCLEAR EXPLOIT KIT.
LET ME PASTE IN THIS.
IT THEN SHOWS YOU'RE NOT RIGHT
AND YOU'RE KICKED OFF.
YOU THINK IT'S A FALSE POSITIVE.
NOW WE HAVEN'T REACHED AN AGE
WHERE THIS IS PREVALENT BUT
WHERE IT HAS BUILT IN SYSTEMS TO
STOP INVESTIGATORS FROM
INVESTIGATING THE ISSUES T-FPLTZ
A GROWN INDUSTRY.
IT'S NOT NEW.
TO GIVE YOU AN EXAMPLE THIS IS A
NICE DIAGRAM.
YOU GO THROUGH A SERIES OF WEB
PAGES AND THEN YOU HIT A LANDING

PAGE.

ANGLER IS A FUN ONE TO LOOK FOR.

THIS IS WHAT IT WOULD LOOK LIKE.

BASICALLY WHAT AUTHORS DO IS

FIND A WEBSITE THAT MAY HAVE

USERS THAT ARE NOT YOU KNOW IS

SECURE.

IN THIS CASE THEY WERE TARGETING

PEOPLE ON THE OBITUARY SECTION.

THEN YOU GET SENT TO SENSE AND

SENSIBILITY.

OVER TO ANGLER IS.

IF YOU ARE VULNERABLE IT WOULD

COMPROMISE YOUR BROWSER AND LOAD

CRYPTO LOCKER.

THERE IS A VIDEO ON THE U TUBE

CHANNEL TO WATCH IT.

WE SELECTED LOGS DURING THE

INVESTIGATION ON THIS.

WE CAN'T BE A HUNDRED PERCENT

SURE.

WE WEREN'T GOING TO WATCH THIS

FOR A YEAR AND ALLOW OUR USER TO

BE COMPROMISED.

ABOUT 90 THOUSANDS PEOPLE ARE

REDIRECTED TO A SINGLE PROXY A

DAY.

THAT HAD 9000 WERE VULNERABLE TO

A EXPLOIT.

WITHIN THE EXPLOIT KIT, TEN

PERCENT, 40% WERE SUCCESSFULLY

COMPROMISED.

40 PERCENT IS A PRETTY HIGH

NUMBER.

OF THE 40 PERCENT, 62 PERCENT

WERE SERVED RANSOM WARE.

THESE NUMBERS PERTAIN TO RANSOM

WARE.

THIS OPERATES THE SAME YEAR OVER

YEAR.

WE KNOW IT'S NOT TRUE.

ASSUMING WE'RE ABLE TO OPERATE

FOR A YEAR.

THIS IS PARTICULAR HOW MUCH

MONEY THEY WOULD MAKE.

THE 2.9 PERCENT I BELIEVE FROM

THE FTC.

NO US CERT.

THINK IT'S CLOSER TO 500 NOW.

THE 147 INVOLVES THE

INVESTIGATION WE HELPED

LIMESTONE OUT WITH.

WE KNOW THE NUMBERS ARE

SIGNIFICANTLY HIGHER.

FROM THE ANGLER PORTION THEY EX

KITED IN THAT FASHION YEAR AFTER

YEAR THEY MADE ABOUT

$34 MILLION.

THERE IS EQUAL IN THE U.S. AND

THE UK.

IT'S LIKELY THEY'RE MAKING

60 MILLION.

MY POINT WITH THIS IS WE'RE NOT

DEALING WITH HACKERS IN THE

BASEMENT.

THESE ARE HACKERS WITH THE

CAPABILITY AND FUNDING OF AN

ATTACK.

THEY ARE TARGETING HUNDREDS OF

PEOPLE.

IT'S GETTING WORST.

UP UNTIL A FEW MONTHS AGO AND

THE SAM SAM CAMPAIGN EVERY PIECE

OF RANSOMWARE REQUIRED A PERSON.

IT REQUIRES A PERSON TO OPEN THE

E-MAIL.

REQUIRED A PERSON TO GO TO THAT

WEBSITE AND NOT HAVE A PATCHED

BROWSER.

IT REQUIRED A PERSON.

IF YOU HAVE A SYSTEM YOU DIDN'T

ALLOW PEOPLE ON YOU WERE SURE IT

WOULDN'T BE INFECTED BY RANSOM

WARE.

THE AUTHORS WERE

UNSOPHISTICATED.

THEY TOOK THE VULNERABILITIES

AND TURNED IT AROUND TO THE

RANSOM DAY A LOAD.

THE VULNERABILITIES WE USE WITH

THE SAM SAM CAMPAIGN.

ONE WAS 7 YEARS OLD.

ONE WAS 9 YEARS OLD.

THESE ARE SERVING SIZE

VULNERABILITIES.

IF YOU HAVE A INTERNET EXPOSED

TO THE INTERNET YOU SHOULD HAVE

SEVERE CONCERNS.

EXPLORES THE SAM SAM CAMPAIGN WE

DECIDED TO SCAN THE INTERNET AND

SEE PARTICULAR HOW MANY MACHINES

WERE OUT THERE.

WE DETECTED 3.5 PH +*L VULNERABLE

MACHINES.

WE FOUND OUT FROM THE SERVICES

ORGANIZATION THEY HAD A CUSTOMER

WHO SAID IT WAS OKAY TO SHARE

DATA WITH US.

WE FOUND OUT THAT BASICALLY IT

THERE IS A PERIOD OF UP TO 74

DAYS WHEN THE SAM SAM

COMPROMISES A MACHINE BEFORE

THEY INSTALL THE RANSOM WARE.

THAT'S GREAT FOR ME.

THEY LOOK FOR THE MACHINES, THEN

SPEND TWO MONTHS DIGGING INTO

IT.

IMMEDIATELY WE WERE ABLE TO WORK

WITH A TEAM TO SCAN THE INTERNET

AND FOUND OVER 2900 COMPROMISED

MACHINES.

WE THEN CONTACTED A PERSON FOR

EACH MACHINE.

WE WERE ABLE TO GET MOST CLEANED

UP AND MOST OF THE BACK DOORS

REMOST.

WHAT DOES THAT MEAN AT THE END

OF THE DAY?

WE WERE LITERALLY ABLE TO TAKE

TENS OF THOUSANDS OF TKHRARBZ

OUT OF THOSE POCKETS.

THE ONLY REASON WHY, THEY USED

OFF THE SHELF COMPONENTS.

NOW THEY HAVE MADE HUNDREDS OF

THOUSANDS OF DOLLARS THEY HAVE

THE FUNDING FOR A DEVELOP TEAM.

THIS HAVE THE FUNDING TO THEIR

OWN BACK DOORS.

THIS IS NO LONGER AN ACADEMIC

THREAT.

IT'S SOMETHING WE SEE IN THE

WILD.

THAT'S ALL I HAVE TO TALK ABOUT

TODAY.

IF YOU WANT TO READ MORE ABOUT

TALOS THERE IS A LINK THERE.

>> THANK YOU, CRAIG.

[APPLAUSE]

>> NOW WE'RE CALLING UP JOE.

WILL HE TALK ABOUT RANSOMWARE

VECTORS.

>> THANK YOU, STEPHEN.

I'M VICE PRESIDENT OF PHISHLABS

IN SOUTH CAROLINA.

WE LOOK AT A TACK VECTORS WHERE

PHISHING IS THE VECTOR.

WE SEE A LARGE MOVEMENT OF

RANSOMWARE.

ONE THING WILL YOU SEE RECURRING

IN OUR CONVERSATIONS.

RANSOMWARE THREAT ISN'T NEW.

IT'S BEEN AROUND FOR A LONG

TIME.

IN FACT THERE IS A GENTLEMAN

WHOSE NAME IS DR. ADAM YOUNG NOW

WORKING AT BLOOMS BERG.

A FRIEND OF MINE.

HE WROTE A BOOK IN 2004, A

CO-AUTHORED BOOK WITH ANOTHER

DOCTOR.

HE POSTULATED THAT BASICALLY

THREAT ACTORS WHO FOCUS ON

CRYPTOGRAPHY COULDN'T DO IT IN

2004 BUT IT WAS A MATTER OF TIME

BEFORE THEY HAD THE RESOURCES.

THERE WEREN'T ENOUGH LABS

AVAILABLE AT THE TIME AND THE

SUPPORTING TECHNOLOGY DIDN'T

EXIST ON A LARGER SCALE.

SINCE THEN WE HAVE SEEN A LOT OF

ADOPTION OF CAMPAIGNS THAT ARE

UTILIZING NOW THE AVAILABLE

CRYPTOGRAPHIC LIBRARIES, TOUR

BASED MESSAGES, P TO P MESSAGING

AND DARK MARKET ARCHITECTURES

BROUGHT UP AND USED AS PART OF

THE DISTRIBUTION CAMPAIGN BY THE

THREAT ACTORS.

NOW YOU HEARD CRAIG TALK LARGELY

ABOUT RANSOM WARE AS A SOCIAL

ENGINEERING CAMPAIGN UNTIL

RECENT SRI.

THAT BEING THE CASE A LARGE

PERCENTAGE OF CAMPAIGNS ARE

DELIVERED WHAT WHICH CONSIDER A

SOCIAL ENGINEER AGO TACK.

THAT IS LARGELY A PHISHING

CAMPAIGN OR GETTING USERS

DIRECTED TO ANOTHER WEBSITE

WHERE THEY HAVE MALICIOUS

VULNERABILITY AND EXPLOITING A

PLATFORM ON THE BROWSER OR

RELYING ON YOU TO DOWNLOAD

MALWARE FROM A SPECIFIC WEBSITE.

WE'RE LOOKING AT EX LIGHTED

DELIVERY.

ADVERTISEMENT CAMPAIGN DELIVERY.

MOSTLY PHISHING E-MAILS.

PHISHING IS LARGELY ACCOUNTS FOR

912 PERCENT OF RANSOMWARE

DELIVERY.

IT'S THE LARGEST OF THE SOCIAL

ENGINEERING TECHNIQUE.

EACH HAS A DIFFERENT TTP, TACTIC

THREAT AND PROCEDURE ASSOCIATED

WITH THE CAMPAIGN IT'S

DELIVERING.

SOME OF THE THINGS WE TALKED

ABOUT OR WE WILL ALL TALK ABOUT

I BELIEVE THAT'S SCARY FOR SUS

NUMBER ONE THE ADOPTION OF THE

ADVANCE ENCRYPTION.

NUMBER TWO THE TECHNOLOGIES THAT

ALLOW FOR COMMUNICATION THAT'S

ARE COMPLETELY ANONYMOUS.

IN FACT WE SAW RANSOMWARE

CAMPAIGNS USING THE RANSOMWARE

COMMUNICATION DELIVERY

PLATFORMS.

BIT MESSAGES THAT IS ENCRYPTION

BETWEEN THE ACTORS AND THOSE

INFECTED.

PAYMENT METHODOLOGIES.

AND OTHER THINGS WE'RE SEEING IS

A IDEA OF TIME LIMITS.

IT USE TO BE PAY US

RANSOMWARE -- PAY US TOMORROW OR

WHICH WILL DELETE YOUR FILES.

WE ZOO THAT A LOT.

OR WE SEE PAY US THE RANSOM BY

TOMORROW OR WE WILL DISCLOSE THE

DATA WE HAVE TAKE FRIEND YOU.

IT'S A PROBLEM THESE DAYS.

ONE OF THE THINGS I WANT TO

HIGHLIGHT HERE IS MALICIOUS

ADVERTISEMENTS.

WHILE IT IS NEW THERE ARE TWO

THINGS I WANT TO SAY.

WHILE IT'S NEW TO THE MEDIA

THERE ARE TWO THINGS TO SAY.

ONE, IT'S NOT UNCOMMON.

IT'S HAPPENED BEFORE.

IT'S BEEN A DELIVERY PLATFORM

FOR A WHILE.

I HIGHLIGHTED AN ARTICLE FROM

MAY 2014 DISCUSSING THE SAME

THING.

THE SECOND THING I WANT TO SAY

ABOUT THE MALICIOUS AD

CAMPAIGNS, NUMBER TWO, THE

REASON WHY PEOPLE ARE SO SCARED

ABOUT MALICIOUS AD CAMPAIGNS IS

THEY'RE DELIVERING RANSOM WARE

TO TRUSTED WEB SITES.

ALRIGHT.

OR WHAT THE USER BELIEVES IS A

TRUSTED WEBSITE.

>> SO THEY RELY ON THE CALMNESS

OF A SITE AND THEN AFFECTED BY

RAM SONWARE.

THE WEBSITE HAS AN ADVERTISEMENT

SCENE WITH MALICIOUS RANSOM

WARE.

>> OKAY LIKE I SAID THE LARGEST

PERCENTAGE IS DISTRIBUTED SROE A

PHISHING.

I'M SURE EVERYONE HAS SEEN A

TYPE OF TP +*EURBGING E-MAIL

BEFORE.

THERE IS A LARGE PERCENTAGE OF

RANSOMWARE OUT THERE.

EACH CAMPAIGN DELIVERS YOU THIS

THROUGH DIFFERENT TECHNOLOGIES

AND METHOD OL KPWAOES.

WE'RE LOOKING AT THIS CRYPT --

PHISHING IS A SOCIAL ENGINEERING

SCAM.

THE USER WILL BELIEVE WHAT THEY

SAY.

THEY WILL CLICK ON A LINK AND

OPEN A A LOAD ATTACHED TOLDT

E-MAIL, RIGHT.

THEY WILL GET THE USER INFECTED

IN ONE WAY, SHAPE OR FORM.

THIS IS CRYPTOWALL IT HAS A

DOCUMENT BUT THE DOCUMENT

DOESN'T CONTAIN AN EXPLOIT.

THERE IS A URL.

WHEN YOU GO TO THE URL IT

DOWNLOADS A PAY LOAD.

IT CAN INSTALL ON THE COMPUTER.

THIS HAS A "DO THE M" FILE A

MICROSOFT TEMPLATE WITH SCRIPT.

WHEN YOU OPEN IT UP IN MICROSOFT

IT EXPLOITS WITH YOU A RANSOM

WARE PAY LOAD.

THIS ISY SEPTEMBERUALLY LOCKY.

THIS IS IN A ZIP ARCHIVE.

IT INFECTS YOU WITH A PAY LOAD.

>> THIS IS RAN -- OOPS

CRYPTOWALL THIS.

IS THE FIRST TARTED SPEAR

TPH +*EURB WHERE THEY'RE

DELIVERING THIS TO THE END USER.

RAN SCAM A SIP FILE ATTACHED

WITH A BATCH FILE ON IT THIS

IS -- IF YOU DON'T KNOW THIS IS

PROLIFIC AS WELL.

THIS IS USING VERY TARGETED

LANGUAGE TO TARGET USERS AND

DELIVERING AN ATTACHMENT THAT IS

INFECTED.

IT'S A FIRST STAGE INFECTER

DOWNLOADED PAY LOADS.

RANSOMWARE BEING A PAY LOAD.

IN ADDITION TO THAT RANSOMWARE

DELIVERS IN OFFICE SCHEMES.

ONE OF THE THINGS MY MARKETING

PROGRAM IS WORKING ON IS A

PUBLIC SERVICE ANNOUNCEMENT

SAYING MACROS AND MICROSOFT

OFFICE IS NOT OKAY.

ANYONE ON THE TABLE WILL TELL

YOU THEY'RE NOT OKAY.

WHAT WE'RE LOOKING AT IS A RAN

SOEPLWARE DOCUMENT WITH AN

ATTACHED FILE.

IT'S EN A +*EUBLZ ABLING THE

MACROS AND IT WILL RUN THE

MALICIOUS SCRIPT AND IT WILL

INFECT YOU.

ONCE THAT OCCURS YOU HAVE RANSOM

PRESENTATION.

THIS IS WHERE THE MAL WARE

AUTHOR TELLS YOU, YOU NEED TO

PAY ME SOME MONEY.

THIS IS A HRARPL NUMBER OF

FLAVORS THE OF -- EACH THREAT

CAMPAIGN HAS DIFFERENT

INFORMATION OR INDICATORS TO

TRACK AND IDENTIFY.

FOR THIS ONE HERE, THIS ONE

HERE, I BELIEVE THIS IS ROKU.

THE THINK ABOUT THIS IS ROKU

ASKED FOR A SMALL PHAOUPBT OF

MONEY AND YOU USE SMALL CODES

WITH A TELEPHONE FOR PAYMENT

EVEN THOUGH THE RANSOMWARE

THREATS ASK FOR SMALL AMOUNTS

PER TRANSACTION LEVELS THEY'RE

STILL SCAMMING HUNDREDS OF

THOUSANDS IF -P MILLIONS FROM

USERS ON A DAILY BASIS.

CAN THIS IS EX TPROEPLLY

INTERESTING.

THE GUYS BEHIND THIS WANT YOU TO

KNOW THEY'RE NOT CROOKS.

THAT YOU CAN RECEIVE YOUR DATA

BACK AFTER SIX MONTHS.

I THOUGHT THAT WAS FUNNY OR PAY

AND RECEIVE IT BACK RIGHT NOW.

>> THIS IS TORN LOCKER.

ONE OF THE THINGS I WANT TO

HIGHLIGHT IS THIS IS NOT THE

FIRMING TIME WE HAVE SEEN THREAT

ACTORS TRY TO DUPLICATE THE TECH

AND PROCEDURES OF OTHER THREAT

ACTORS.

THEY'RE TELLING YOU WE'RE CRYPTO

LOCKER WITH THE SAME RANSOM TEXT

AND THE SAME DUPLICATE PAGE

VERBIAGE AND LETTING THE USER

KNOW YOU HAVE TO PAY US.

MAKING THEM THINK THEY'RE INFECT

THE DIFFERENTLY.

PETYA DOUBLE THEIR FINE AFTER A

CERTAIN AMOUNT OF TIME.

JIGSAW WHICH IS SCARY.

IF YOU DON'T A WITHIN -- IF YOU

REBOOT THEY DELETE A THOUSAND

FILES.

EX TREATMENTLY SKAEY.

THERE IS ZEPTO ASKING FOR A

SMALL A MOWN LIKE $1500.

IN A RANSOM WARE LIFE CYCLE WE

HAVE A PHISHING DELIVERY AND

THAT TKAEUBGZ TO YOU A PAGE

DELIVERING A PAY LOAD OR SCAM TO

THE USER.

IT'S NOT MARKED TO A SPECIFIC

BRAND.

ONCE THAT OCCURS AND THEY INFECT

A USER THEY BRING THEM TO A

RANSOM PAGE.

THIS SAYS THIS IS HOW YOU PAY

THE BIT COIN.

AND THEY LIKE TO MIMIC OTHER

RANSOMWARE SCAMS.

IN THIS EXAMPLE CRYPTO LOCKER

WITH.

THAT I THINK I SET THE STAGE.

>> THANK YOU.

>> THANK YOU.

JOE.

>> NOW WE WILL CALL UP LANCE.

LANCE WILL GIVE US INSIGHTS INTO

WHO LIKELY IS BEHIND RANSOMWARE

AND DISCUSS HOW LOW END

CRIMINALS CAN GET INVOLVED USING

WHAT IS OFTEN CALLED RANSOMWARE

AS A SERVICE.

>> GOOD MORNING.

EVERYBODY AWAKE.

ALRIGHT, COOL.

ALRIGHT.

SO, I'M LANCE JAMES.

I'M OVER AT FLASHPOINT.

JUST KIND OF GLAD TO BE HERE.

WE TALKED ABOUT TECHNIQUES --

AND PROCEDURE.

WE'RE LOOKING AT SPECIFIC

RUSSIAN RANSOMWARE CAMPAIGN AND

RELATIONSHIPS WITH OTHER

CRIMINALS OR A FLIP YEATS IN THE

CRIMINAL ORGANIZATIONS AND HOW

THEY RECRUIT OUT AND DOUBLE UP

MONEY ANOTHER ONE WE TALK ABOUT

HOW THE BAR IS LOWERED.

WE ARE SEEING RANSOMWARE THAT

YOU DON'T EVEN NEED CODE.

THERE IS RANSOM32.

YOU PUT IN SETTINGS AND YOU HAVE

YOUR OWN RANSOMWARE.

IT'S A COMMON COMMODITY TOOL FOR

BUSINESS.

A FASCINATING FACT ON THE HIGHER

TIERED ORGANIZATION SUCH AS MAZA

AND EXPLOIT, THE TOP TIER, RICH

CRIMINAL RUSSIAN CRIMINALS OUT

THERE HATE RANSOMWARE.

THEY BELIEVE IT'S DESTROYING THE

INTELLECT I'LL GAME AS AS

HITTERRING THE BUSINESS WITH TOO

MUCH ATTENTION.

IF I MAY QUOTE, THERE WAS A

QUOTE OFF A FORUM WE SAW "I HOPE

THAT EVERY RANSOMWARE FAMILY

ENDS UP IN THE HOSPITAL, AND THE

MACHINE THAT KEEPS THEM ALIVE

GETS INFECTED WITH RANSOM WARE"

THAOEFPLTZ ARE THE FEELINGS OF

HIGHER TIERED BUSINESSES WITHOUT

THE LIGHT ON THEM.

AS WE HAVE SEEN EARLIER WE

TALKED ABOUT SAM SAM.

HEALTHCARE IS A LUCRATIVE

TARGET.

SO, ONE OF THE THINGS RANSOM

WARE AS A SERVICE IT ENABLES

AFFILIATES FROM OUR KING PINS OR

CEOs ON THE OTHER SIDE OF IT.

SO SIMILAR TO CRYPTO LOCKER.

HOW IT WORKED WITH.

WE SEE ANGLER EXPLOITS.

THERE ARE INDIVIDUALS, PIECES

WHERE THEY GET THE MALWARE ONTO

THE COMPUTE EURZ.

ON THE LOWER END SIDE.

A LOT OF THE LOWER END TIERED

CRIMINALS DON'T HAVE ACCESS TO

THE HIGH END DISTRIBUTION

CHAINS.

THEY PW +*LTD BUILD OUT THEIR

AFFILIATES AND FIND OUT THAT

THEY ATTRACT EACH OTHER NOW WE

HAVE LOW END CRIMINALS.

MY CONCERN IS HIGHER MAKING UP

TO $34 MILLION IN A SHORT AMOUNT

OF TILE.

AS THIS IS MORE COMMONPLACE THE

QUESTION IS MORE AND MORE PEOPLE

PAY THE RANSOM WHAT HAPPENS WHEN

IT'S NOT ABOUT THE RANSOM.

IT'S COERCION OR OTHER TECHNIQUE

TO GET SPH-L DONE IN THE .

SO, THIS IS BASICALLY A

RECRUITMENT METHOD HERE.

THEY GET THE SLIDES.

THE CAMPAIGN BOSS REACHED OUT

AND APPROACH -DZ A LOW SCALE

CRIMINAL AND SAYS I WILL GIVE

YOU 40 PERCENT.

YOU GET THIS MAL WARE ON

EVERYONE'S COMPUTER.

WHAT WILL HAPPEN THERE IS THE --

THEY ATTRACT AN AFFILIATE DOING

IT BOTNET IN STALLS AND GET IT

PROPAGATION.

SO THIS AFFILIATE GOES OUT AND

CHASES ACCESS TO THE COMPUTERS.

SO IT'S MORE LOW KEY.

LESS SOPHISTICATED.

IT'S WHO DO YOU KNOW, HOW DO YOU

GET ACCESS INTO IT.

>> THEY ALSO DO LOADING

RANSOMWARE ON COMPROMISED

SYSTEMS.

E-MAIL AND SOCIAL MEDIA SPAM.

SPAM BOTNETS TO DISTRIBUTE

SPAMWARE.

COMPROMISED DEDICATED SERVICES

FOCUSING ON.

BRUTE FORCING AN STEALING

CREDENTIALS FROM BOT NET LOGS.

EVEN DATING AND TOURING OTHER

SITES AND FILE SHARING WEB SITES

ARE ACTIVE TO EXPLOITING AND

TRICKING PEOPLE TO CLICK ON

SOMETHING AND IT'S RANSOM WARE.

>> THESE ARE MORE ATTRACTIVE FOR

THINK TO CLICK ON AND IT'S

RANSOM WEAR.

YOU HAVE THE RAM SON WEAR BOT.

HE REACHED OUT TO THE AFFILIATE

AND SAYS, GET THIS MOVED OUT.

ALRIGHT.

THEN THE AFFILIATE GETS THIS

DISTRIBUTED.

IT'S NOT A LOT THESE ARE LOWER

TIERED.

THEN THE I FECTED PERSON GETS

THE NOTICE.

THEN THE BOSS REACHED OUT AND

DOES THE KPHOUP CATION FOR THE

TRANSITION.

NOT THE AFFILIATE.

THE AFFILIATE FOCUSES ON

DISTRIBUTION, RIGHT.

ONCE THAT IS DONE AND THE BOSS

IS PAID THE BOSS AS THE

AFFILIATE 40 PERCENT OF THE

100 PERCENT ON THAT.

THAT CONTINUES ON THE CYCLE.

SO, WHAT WE SEE THOUGH IS A LOT

OF SCHEMED SCENARIOS.

IT BASICALLY DROPS DOWN TO LOW

LEVEL.

THE BIG COIN PAYMENT.

THEY ENCRYPT.

DO THE 40 PERCENT.

SOME CRIMINAL BOSSES WILL ASK

FOR MORE MONEY AND SAY I HAVE

YOU AGAIN OR I WANT MORE.

THEY WANT MORE TAKE.

THEY DON'T LIKE THE 40 PERCENT

BUT NODE TO ATTRACT PEOPLE TO DO

THIS.

SO THE MONEY FLOW IS SIMPLE.

THIS WAS MENTIONED EARLIER HOW

WE GOT FROM THE AIDS VIRUS TO

THE RANSOMWARE VIRUS NOW IS

THROUGH THE FLOW OF BITCOIN.

ALMOST UNTRACEABLE WE SEE A

CONSIDER AMOUNT OF ACTIVITY.

BIT COIN IS RECEIVED FROM THE

VICTIM BASICALLY.

THEY TAKE THE BIT COIN RECEIPTS

AND GO THROUGH BIT COIN -- AND

LAUNDER IS.

THEY THEN HAVE A CLEAN WALLET.

THE WALLET'S THAT MAYBE INVOLVED

ARE NOT ASSOCIATED.

>> THEN FORWARDS THE REST.

THIS AND A FEW WE HAVE SEEN

HERE, THE AVERAGE OF THE LOW

TIER.

THEY MAKE ABOUT A HUNDRED

THOUSAND A YEAR, 90,000 A YEAR.

IN RUSSIA THAT'S NOT BAD THOUGH.

SO, ON AVERAGE THEY MAKE $7500 A

MONTH.

THEY HAVE A LIFETIME -- WE DID A

LIFE PATTERN HERE, AN IDEA

HEREOF THEIR BUSINESS.

ON AVERAGE WE SEE, SORRY -- IT'S

HARD TO SEE.

THE AFFILIATES AVERAGE TAKE HOME

SALARY IS ABOUT 600.

THE FORM ACCOUNT PER VICTIM IS

$300.

SO, IT'S ACTUALLY A LOW PRODUCT

RANGE.

IT DOESN'T MEAN IT WON'T

CONTINUE TO GROW.

THE PROBLEM WITH TODAY'S RAM SON

WARE YOU DON'T KNOW IF IT'S

USING THE BIT.

IF IT'S CRYPTO LOCKER OR

SOMETHING OF THAT VARIANT.

YOU KNOW THE COMPUTER STOPPED.

CAN'T DO BUSINESS AND YOU HAVE

TO PAY THE PERSON.

A LOT ARE SIMPLIFIED.

NOT COMPLICATED.

MANY CASES SECURITY TEAMS CAN

BREAK SOME OF THE LOWER TIER

ONES.

WE SEE WITH THE HIGHER TIER ONES

THEY'RE COPYING AND SEEING THE

BENEFIT OF UTILIZING NATIVE

DESIGNED KRIT TOP IN THE MAL

WEAR.

THIS IS JUST A GROWING PROBLEM

THERE.

KEY FINDINGS TO THIS IS THE

BARRIER IS LOW.

THAT'S A FACT.

YOU CAN GET IT ANYWHERE THESE

DAYS, BUSINESS OR HOME.

THE RUMOR AS IT'S MORE KPHOD

COMMODITY.

THE $30,000 THINGS IS RARE.

IT'S NOT ALWAYS TO ONE PERSON.

WE SEE THE CAMPAIGNS CRYPTO WALL

AND CRYPTO LOCKER.

WE WILL SEE SMALLER CAMPAIGNS

NOW FOR EVERYONE TO GET IN.

THE MONEY WILL BE SPREAD OUT.

WELCOME TO THE WILD WILD WEB.

THE DAYS OF 30 MILLION ARE LESS

OF A COMMON GAIN, AND MORE

SPREAD OUT.

STANDARD LIVING OF A HUNDRED

THOUSAND DOLLARS A YEAR OR . SO

THANK YOU.

>>

[APPLAUSE]

>> THANK YOU, LANCE.

AND FINALLY ON OUR PANEL WE HAVE

GEORGIA.

GEORGIA WILL DISCUSS EMERGING

RANSOMWARE THREATS WITH RESPECT

TO MOBILE DEVICES AND OTHER

CONNECTED DEVICES.

>> SERIOUSLY IF YOU'RE GETTING

ON THIS STAGE LATER BE CAREFUL.

EVERY TIME I STOOD UP I HAVE

ALMOST GONE OFF THE BACK OF

THIS.

I GUESS THAT WOULD BE A GOOD WAY

TO MAKE A ENTRANCE.

YOU KNOW, SO, EITHER YOU'RE

MAKING $30 MILLION OR 90,000 A

YEAR.

YOU KNOW IF YOU HAD A START UP

YOU KNOW $90,000 A YEAR SOUNDS

PRETTY NICE.

OBVIOUSLY I'M IN THE WRONG

BUSINESS AND SHOULD MAKE

RANSOMWARE.

SO I'M GEORGIA.

I AM FOUNDER AND CTO OF A

COMPANY CALLED SHEVIRAH.

WE ARE EQUIPPING PENETRATION

TESTERS TO TEST INTO MOBILE AND

INTERNET OF THINGS.

THE IDEA IF THIS IS GOING TO

HAPPEN TO YOU, RANSOMWARE YOU

CAN TEST THE RISK AHEAD OF TIME.

SO, I DO A LOT OF SIMULATING,

BAD ACTSERS.

I'M NOT A BAD GUY, I JUST PLAY

ONE ON TV, IF YOU WILL.

WE WILL TALK ABOUT WHERE MALWARE

AND PARTICULARLY RANSOMWARE IS

HEADING.

PARTICULARLY MOBILE AND INTERNET

OF THINGS.

UNLIKE THESE THINGS HAVE FACTS.

I'M TALK ABOUT THE FUTURE I

BASICALLY GET TO MAKE IT ALL UP.

TAKE IT WITH A GRAIN OF SALT IF

YOU WANT TO.

ANYWAYS MOBILE RANSOMWARE.

AS RANSO MANY WARE GETS BIGGER

NOBLE DOES TOO.

MOBILE DEVICE IS THE PERFECT

THING TO GET.

IT'S IN MY POCKET NOW.

IT'S ALWAYS WITH ME LITERALLY

ALL THE TIME.

SO, WE HAVE SEEN A LOT ALREADY.

LIKE WE HEARD IN PREVIOUS TALKS

NOT ALWAYS PARTICULARLY

SOPHISTICATED.

THINK RANSOM WARE GETS THAT BAD

VIBE THAT IT'S SO COMPLICATED

AND YOUR COMPUTER WILL NEVER

RECOVER FROM IT A LOT OF TIMES

IT'S SIMPLE AND IT'S ASKING

PEOPLE, LIKE DO YOU WANT TO MAKE

ME A DEVICE ADMINISTRATE TORE

DAY.

I'M JUST AN APP FOR THE PHONE

THAT PLAYS GAME BUT I SHOULD

HAVE ADMINISTRATIVE PRIVILEGES.

SURE.

THEN IT CHANGES THE PIN OR SETS

THE PIN SO YOU CAN'T LOG NO YOUR

PHONE.

YOU HAVE TO PAY THE RANSOM TO

GET IT BACK.

WE HAVE SEEN THINGS WHY WAS IT'S

AN OVER LAY.

MY APP IS ALWAYS ON TOP.

NO MATTER WHAT.

YOU CAN'T DO ANYTHING ELSE ON

THE PHONE.

YOU HAVE TO PAY TO BASICALLY

MAKE THE OVERLAY GO AWAY.

LIKE I SAID IT'S NOT VERY

SOPHISTICATED AT ALL BUT PEOPLE

PAY.

THAT'S WHAT WE HAVE SEEN SO FAR.

IF YOU THINK ABOUT MOBILE IT

COULD GET WAY WORST.

THINK ABOUT THE THINGS ON YOUR

PHONE.

ALL OF THE THINGS YOU DO WITH

YOUR PHONE.

ALL OF THE THINGS YOUR PHONE

COULD DO.

LIKE I GUESS A FEW YEARS AGO

NOW, WE SAW THE CELEBRITIES WITH

THEIR NUDES UP LOADED TO

ICLOUD AUTOMATICALLY.

CELEBRITIES ARE NOT THE ONLY

ONES THAT DON'T WANT THAT TO

HAPPEN.

YOUR PHONE HAS PHOTO, AUDIO AND

VIDEO RECORDING.

YOUR PHONE IS WITH YOU

EVERYWHERE.

I KNOW I TAKE MY PHONE IN THE

SHOWER WITH ME.

DON'T YOU.

CERTAINLY CELEBRITIES ARE NOT

THE ONLY ONES WHO DON'T WANT

THAT TO HAPPEN.

A NEW RANSOMWARE.

WE'RE RELEASING THESE VIDEOS WE

TOOK IF YOU DON'T PAY US THE

MONEY.

THE PHONE SETS UP.

LAP TOPS WITH THE GREEN DOT HAVE

THAT AS WELL.

YOUR PHONE IS MORE AOU BIC AOU

UBICOTOUS.WE WILL SEE MORE AND MORE OF IT.

WHY WE WILL SEE MORE OF IT IS

BECAUSE IT'S EARLY AS 2014 WE

WERE SELLING MORE MOBILE DEVICES

THEN LAP TOPS.

YOU KNOW SALES WISE.

YOU KNOW YOU PROBABLY THINK BACK

TOE YOUR OWN BUYING HISTORY IT'S

PROBABLY STEW TRUE.

YOU HAVE TONS OF THINGS

QUALIFYING AS A MOBILE DEVICE.

A FANCY NEW iPAD EVERYONE HAS

TO HAVE ONE.

THEN THE BOSS GETS ONE AND IT

TRICKLES DOWN.

WE AS SECURITY PEOPLE HAVE TO

PUT THEM ON THE NETWORK.

SO, THAT'S WHERE.

THE BAD GUYS GO WHERE THE MONEY

IS.

AS THERE ARE MORE DEVICES OUT

THERE, MORE POTENTIAL TARGETS

AND RITCHER TARGETS.

NOW WE HAVE, YOU KNOW ALL OF OUR

WORK DOCUMENTS ON THERE.

GOOGLE DOCS, OFFICE SUITE,

E-MAILS, PICTURES, PERSONAL AND

PROFESSION LIVES COMPLETELY ON

THESE DEVICES.

THEY'RE PROBABLY THE BEST TARGET

THEY COULD BE.

CERTAINLY THAT WOULD BE WHERE I

WOULD WANT TO GO.

MAYBE THAT'S WHY I MADE A

COMPANY AROUND IT.

SO WHY IS MOBILE DIFFERENT.

YOU MAY THINK THAT YOUR PHONE

REALLY ISN'T THAT DIFFERENT FROM

YOUR COMPUTER.

YOU WOULD BE RIGHT IN A LOT OF

WAYS.

ANDROID OR iOS OR WINDOWS

MOBILE OR THE BLACKBERRY.

THEY'RE A COMPUTER THAT GOAT

SMALL.

THEY HAVE ALL OF THE SAME

CAPABILITIES AND THEN SOME.

& RANSOM WHERE IT MAKES THINGS

HARDER.

WE HAVE PUT IT IN PEOPLES HEADS.

DON'T CLICK ON LINKS AND

E-MAILS.

NOBODY HAS SAID ANYTHING ABOUT

LINKS AND TEXT MESSAGES.

DON'T CLICK ON LINKS AND

TWITTER.

DON'T CLICK ON LINKS IN

WHAT'SAPP AND POKEMON GO.

WE HAVEN'T DONE.

THAT MY FAVORITE QUOTE AROUND

THIS.

THE GUY THAT TOLD ME IS IN THE

ROOM.

HE SAID LINKS ARE MEANT TO BE

CLICKED.

IT MAKES IT DIFFICULT WE SAY ONE

SET OF LINKS IS BAD.

IN GENERAL -- WE THINK ABOUT THE

THINGS THAT YOU ARE SUPPOSE TO

LOOK FOR.

IF YOU ARE GOING TO CLICK ON A

LINK.

YOU LOOK ON YOUR E-MAIL.

IT TELLS YOU TO HOVER OVER IT WE

SHOW YOU THE FULL LINK.

WE THEN SEE THE LINK ON THE

CORNER IT'S HTTPS.

THAT'S WHAT YOU'RE TAUGHT TO DO

IN SECURITY AWARENESS.

HOW DO YOU HOVER OVER A LINCOLN

A PHONE.

YOU DON'T, RIGHT.

WHAT DO YOU DO?

THEN AGAIN YOU HAVE OUT OF BAND

WAYS TO COMMUNICATE.

WHAT HAPPENS TO SOMEONE YOU KNOW

SENDS YOU A MESSAGE ON FACEBOOK

MESSENGER WITH A LINCOLN IT

CHANCES ARE IT'S SOMEONE YOU

KNOW OR IT HAS THEIR PICTURE AND

YOUR FRIEND.

WHAT DO YOU DO?

I THINK THAT -- IT'S DIFFICULT,

EVEN AS SOMEONE WHO DOES

SECURITY FOR A LIVING TO SAY I

WILL USE THE INTERNET AND MY

TECHNOLOGY SECURITILY TODAY.

I DON'T THINK I MAKE IT PAST

MAYBE BREAKFAST BEFORE I HAVE

DONE SOMETHING INSECURE THAT

WOULD MAKE ME POTENTIALLY A

TARGET TO THESE THINGS.

WHAT IS WORST FOR US WITH

COMPANIES.

WE CAN'T REALLY DO THE SAME SORT

OF THINGS AROUND MOBILE THAT WE

DO AROUND LAP TOPS.

IF I GIVE MY EMPLOYEES LAP TOPS

I HAVE A LOST SAY OF THE

PROGRAMS ON THERE.

THE PATCH LEVELS, THE

REQUIREMENTS FOR PASSWORDS.

WE ARE MOVING IN THE RIGHT

DIRECTION WITH MOBILE BY DEVICE

ADMINISTRATION, ENTERPRISE

MOBILITY MANAGEMENT.

THINGS LIKE.

THAT IN GENERAL IT'S STILL THE

USERS DEVICE.

THEY MAY GIVE TO T. TO THEIR

KIDS ON THE WEEKEND TO DOWNLOAD

GAMES.

YOU KNOW, SOME OF YOU PROBABLY

KNOW HOW EXPENSIVE THAT CAN BE.

THAT'S RANSOMWARE ALL BY ITSELF,

RIGHT.

SO, I MEAN WE HAVE A LONG WAY TO

GO.

MOBILE CAME UP LATER, WE ARE

STILL A LITTLE BEHIND IN

SECURITY IN A LOT OF WAYS.

PARTICULARLY AROUND USER

AWARENESS.

I THINK WE HAVE MADE A BIG DENT

IN THE USER AWARENESS PROBLEMS

AROUND MOBILE PHISHING BUT WE

HAVE FARTHER TO GO.

SO, I THINK THAT'S WHY IT'S SUCH

A GREAT TARGET.

THERE IS NOT MUCH OUT THERE FOR

IT YET.

IT'S NOT JUST MOBILING.

THINK ABOUT THE THINKS LIKE

CONNECTED CARS, EVEN

TELEVISIONS.

CERTAINLY YOU HAVE PROBABLY

HEARD THAT A LOT OF THE SMART

TVs HAVE A MICROPHONE THAT IS

LISTENING ALL THE TIME.

PARTICULARLY THOSE WHO LIVE IN

THE DISTRICT HAVE SMALL

APARTMENTS THAT MAY MEAN

SOMETHING TO YOU.

THEN IT CAN BE THINGS LIKE TOYS.

LIKE HELLO BARBIE THAT HAVE A

WiFi CONNECTION AND A

MICROPHONE IT WAS RECORDING

CHILDREN ALL THE TIME.

AS LONG AS IT HAS A INTERNET CON

CONNECTIVITY IT HAS THE ACT TO

BRUISE THE INTERNET, AN

OPERATING SYSTEM, A WAY TO

COMMUNICATE WITH THE USER.

IT COULD BE FOR RANSOMWARE AS

WELL.

WE SAW AT THE DEATHCON

CONFERENCE RESEARCHERS DID A

HOME THERMOSTAT WITH RANSOMWARE

MAYBE THEY WOULD MAKE YOUR HOUSE

REALLY HOT OR COLD, MAKE THE

AIRILY AND RUN UP THE BILL.

THINK ABOUT THE DAY MY CAR WON'T

START AND THE RANSOMWARE COMES

UP ON THE LITTLE SCREEN WHERE

THE MUSIC SUPPOSE TO PLAY AND

SAYS PAY ME MONEY OR I WON'T

START YOUR CAR TODAY.

THAT'S THE REALITY OF WHERE

WE'RE HEADED.

IT GIVES US THE ABILITY TO HAVE

OUR CARS POTENTIALLY DIAGNOSED

OVER THE INTERNET TO FIX THEM

FOR US BEFORE WE EVEN DRIVE INTO

THE PLACE.

THEN WE'RE OPENING IT UP TO A

LOST OTHER MALICIOUS PEOPLE.

YOU KNOW YOU HAVE TO TAKE THE

INTERNET OF THINGS, THE

POSSIBILITY THAT RANSOM WARE MAY

COME.

SO, WHAT DO YOU DO?

DON'T CLICK ON ANY LINKS EVER.

DON'T USE BROWSERS.

DON'T USE TECHNOLOGY.

DON'T RUN A WEB SERVER.

THEN YOU'RE JUST IN TROUBLE.

IN ALL SERIOUSNESS YOU HAVE TO

TAKE INTO ACCOUNT THIS MAY

HAPPEN TO YOU.

YOUR KWOEL IS GOING TO BE TO

MITIGATE YOUR RISKS AROUND IT.

THINK THE ONLY WAY AS A SECURITY

PERSON I GET THROUGH MY DAY

WITHOUT SHATTERING INTO NOTHING

I JUST HAVE TO THINK OKAY NO

MATTER WHAT I DO THE RISK IS OUT

THERE.

I HAVE TO MAKE IT SO IF IT

HAPPENS TO ME AND I AM A VICTIM

OF RANSOM WARE I WILL HAVE MY

STUFF BACKED UP.

I WON'T HAVE MY CUSTOMER DATA ON

THERE FOR THEM TO RELEASE.

STUFF LIKE.

THAT TAKE INTO ACCOUNT THESE

RISKS DO VERY MUCH EXIST AND

THERE ARE WAYS YOU CAN LIMIT

YOUR RISK BUT YOU WILL BE

SOMEWHAT SUSCEPTIBLE TO THEM.

IF YOU'RE A MEMBER OF MODERN

SOCIETY.

SO, THAT'S ME.

I GUESS THAT'S NEXT.

[LAUGHING]

[APPLAUSE]

>> THANK YOU, GEORGIA.

>> WE HAVE TIME FOR A COUPLE OF

QUESTIONS.

WE HAVE ONE QUESTION AND ANOTHER

ONE JUST POPPED UP.

SOME OF THE PRESENTATIONS

HIGHLIGHTED MALICIOUS AD

CAMPAIGNS.

OUR QUESTION HERE IS ARE THERE

THINGS THAT LEGITIMATE PLAYERS

IN THE AD ECHO SYSTEM SHOULD BE

DOING TO PROTECT CONSUMERS FROM

MALV ERTISING.

ANY THOUGHTS FROM THE PANEL.

CRAIG.

>> YA, I THINK ONE OF THE -- CAN

YOU HEAR ME.

I THINK ONE OF THE FIRST THINGS

IS VET ADS.

MAKE SURE THEY COME FROM A

TRUSTED SOURCE.

ANOTHER THING IS CRACKING DOWN

ON THE WAY AD EXCHANGE IS

CURRENTLY ALLOWING ADS TO TRADE

PLACES FOR VARYING AMOUNTS OF

MONEY.

IT'S NOT DIFFICULT TO MAKE SURE

THEY ORIGINATE FROM A SINGLE

SITE OR THAT SITE IS TRUSTED.

IF YOU SEE YOU KNOW AN AD FOR A

PRODUCT IN THE UNITED STATES AND

IT HAS A LINK TO A EASTERN

EUROPEAN SITE AND YOU KNOW KNOWN

REPUTATION THAT SHOULD BE A FLAG

AND SOMETHING TO BE LOOKED INTO.

>> IS I WILL MAKE A COMMENT.

I THINK IT'S IRONIC RANSOMWARE

USED -- YOU COULD BUILD AN

ADVERTIFICATION SYSTEM THIS IS A

SIGNED AD THAT'S THE FUTURE OF

THE WAY TO DO IT EVEN THOUGH IT

COULD OF BEEN DONE YESTERDAY.

>> I THINK THE REALITY IS RIGHT

NOW THE VIABLE OPTION FOR USERS

IS TO BLOCK ADS.

DOING IT ISN'T IN THE ECONOMIC

INTEREST OF THE AD PROVIDERS.

UNTIL THEY INVEST TO MAKE IT

SECURE AND PROVIDE IS THAT CHECK

OF SECURE ADS.

>> LIKE A UL.

TO GET SOMETHING TO PLUG INTO

THE WALL.

YOU HAVE TO GET THERE.

YOU HAVE TO PASS SPECS.

MAYBE WE SHOULD DR. SOMETHING

LIKE.

THAT.

>> I WAS GOING TO ADD TO THIS

IT'S NOT JUST ABOUT BLOCKING

ADS.

THERE ARE SEVERAL INSTANCES WE

SEE WEB SITES ARE SERVING UP

MALICIOUS SCRIPT AND DETECT,

THEY DETECT THE AD BLOCKER.

THEY WILL POP UP MESSAGES ON THE

SCREEN MUCH LIKE INJECT TPHAOGT
BROWSER SESSION TO SAY YOU'RE
USING AN AD BLOCKER DISABLE THE
AD BLOCK TORE VIEW THIS SITE.
WHAT YOU SEE IS YOU SEE THE USER
WANT TO GO TO THE PAGE.
THEY'RE SAYING OKAY I WILL
DISABLE IT TO GO TO THIS PAGE.
THEN ESSENTIALLY YOU'RE GOING TO
A MALICIOUS SITE.
>> IN A NUTSHELL HE'S SAYING, A
BRILLIANT OBSERVATION.
THESE WEB SITES KNOWN TO BE
HOSTING MALICIOUS ADS FORCE THE
USEERS TO DOWN GRADE SECURITY TO
USE THE SITE.
>> WE WILL ALL DO IT, RIGHT?
EVEN AS AWE AN ADVANCE SECURITY
PERSON, SO TO SPEAK.
>> IF WHAT IS ON THE OTHER SIDE
IS SOMETHING WE REALLY WANT OR
NEED WE'RE DEFINITELY GOING TO
DOWN GRADE SECURITY TO GET THERE

BE IT INSTALL JAVA OR TURN OFF

THE AD BLOCKER.

>> I THINK IT'S A MATTER OF

CONVENIENCE OVER SECURITY.

SECURITY VETERAN WILL LET YOU

KNOW IF I WANT SOMETHING LUB

SURPRISED WHAT I WILL DO.

I HAVE A NEW JAVA UPDATE.

>> I THINK IT WILL BE LESS

CONVENIENT TO TURN OFF AN AD

BLOCKER.

I DON'T KNOW HOW TO DO IT.

>> OKAY.

I WILL TRY TO COMBINE TWO

QUESTIONS.

SOMEWHAT SIMILAR.

I WILL TRY TO COMBINE THEM INTO

ONE QUESTION.

>> HOW DOES RANSOMWARY FECT

CONNECTED BACK UPS.

CAN PRACTICES BY THE CONSUMER

BUSINESSES INSURE THE BACK UP IS

NOT INFECTED.

CAN RANSOM WARE ENCRYPT FILES

STORED IN THE CLOUD?

A LOT OF BACK UP IS IN THE

CLOUD.

OR DOES IT ONLY REACH FILES

STORED LOCALLY ON A SERVER.

>> SO, RANSOM WARE THERE HAS

BEEN STUFF THAT GOES AND

ATTACKS.

IT'S NOT AS MANY, YOU KNOW

THINGS HAVE GONE TO ATTACK THE

BACK UP SYSTEM OR DEAL WITH.

THAT

SPEAKING OF THE FUTURE IT'S THE

ONLY NEXT OPTION THAT THEY WILL

HIT UP.

IT COMES DOWN TO THE CLOUD

QUESTION, NO NOTHING WE HAVE

SEEN DO THAT.

YOU HAVE TO HOLD THE CLOUD AS A

DUAL HOST SYSTEM.

THEY HAVE TO HACK THAT AND THE

RANSOM WARE.

THE TIMING WOULD BE IMPECCABLE.

ON THE REALITY OF THE CONNECTED

BACK UP A LOT OF THE TIMES IT'S

VERY, THE THE IDEA OF A BACK UP

IS SOMEWHERE YOU STORE.

LIKE THE OLD WAY OF DOING A BACK

UP YOU STORE IT SOMEWHERE.

AN ARCHIVE OFF SITE OR AWAY FROM

YOU.

THINK ABOUT IT AS IF A BURGLAR

GETS IN THE HOME THERE.

IS AN INVENTORY IN YOUR HOME YOU

DON'T WANT STOLEN.

YOU GET A SAFE DEPOSIT BOX.

JEWELRY OR WHATEVER IT IS.

YOU MAY SAY MY HOME GET BROKEN

INTO.

THEY DIDN'T KNOW ABOUT THE SAFE

DEPOSIT BOX.

THEY DIDN'T GET THERE.

YOU HAVE TO TREAT IT MORE LIKE.

THAT IT'S NOT PERFECT OBVIOUSLY.

I HAVE A TIME MACHINE BACK UP ON

MY MAC iOS.

I HAVE A COPY ON A SEPARATE SSD

HARD DRIVE I CAN HAVE.

I HAVE A REMINDER THAT TELLS ME

TO DO IT ONCE A WEEK.

>> I THINK IT'S ABOUT THE

TECHNOLOGY THAT'S BEING UTILIZED

IS PART OF THE INFRASTRUCTURE OF

THE USER.

WHAT I MEAN BY THAT IS, I HAVE

SEEN A LOT OF MALWARE SAMPLES

NUMERATE FILE SHARING FOR

EXAMPLE.

IF IT'S YOUR F DRIVE, FOR

EXAMPLE.

ESSENTIALLY IT'S ENUMERATING THE

HARD DRIVE.

IF THE F DRIVE IS A MAP TO THE

NETWORK IT WILL ATTACK THE FILES

ON THE NETWORK SHARE.

SAME WITH THE CLOUD SERVICES ON

A CONSUMER LEVEL.

IF IT'S TECHNOLOGY DROPBOX OR

GOOGLE DRIVE THAT HAS A HOSTED

DRIVE ON YOUR COMPUTER.

IT'S VULNERABLE TO THE ATTACK.

ONCE THE CHANGES ARE MADE ON THE

OPERATING SYSTEM.

THE CHANGES RENEXT IN THE CLOUD

SERVICE.

>> A LOT OF PEOPLE DON'T REALIZE

THAT.

>> THAT MAKES SENSE.

>> IF IT'S A LEGITIMATE BACK UP

YOU CAN'T CONNECT IT TO THE

SYSTEM.

WE SEE MAL WARE THAT DIDN'T DO

THIS.

NOW WE SEE MORE MALWARE DOING

THIS.

GREAT EXAMPLE THE WINDOWS BACK

UP SYSTEM.

THOSE WERE LEFT IN PLACE AND

COULD RESTORE FROM IT SLOWLY BUT

SURELY ALL RANSOMWARE IS HITTING

THAT AS WELL.

>> I DIDN'T THINK ABOUT DROPBOX

AS A BACK UP SERVER.

IT SHOULDN'T BE.

>> DON'T JUDGE ME.

>> NO, IT'S TRUE PEOPLE USE IT

FOR.

THAT.

>> YES ABSOLUTELY.

>> IF YOU CONSIDER THE LARGEST

PERCENTAGE OF PEOPLE USING

COMPUTERS ARE CONSUMERS.

THEY'RE HIT WITH RAN SOME WARE.

>> FROM THE POINT OF THE FUTURE

I THINK WHAT I HAVE STARTED TO

SEE IF YOU GET YOUR MOBILE

DEVICE INFECTED NATURALLY YOU

WILL PLUG IT INTO THE COMPUTER

THE OLD SCHOOL WAY OF BACK

UNDERSTAND OR TO CHARGE THE

THING.

IT'S A GOOD WAY TO PIVOT FROM

ONE DEVICE TO THE OTHER.

GET ACCESS ONE DEVICE.

IT'S ON THE HOME NETWORK OR
CORPORATE NETWORK AND TRIES TO
ATTACK OTHER DEVICES OR
PHYSICALLY PLUGGED INTO ANOTHER
DEVICE AND TALK TO THAT TO
INFLECT ANOTHER DEVICE.
IT WAS SAID, SERVICES ALWAYS
LOGGED IN SERVICES AROUND MOBILE
THOUGH.
CERTAINLY WE SEE THEM ON OUR LAP
TOPS AS WELL.
IF THE DEVICE IS LOGD IN.
I HAVE ACCESS TO THE DEVICE THEN
I CAN POTENTIALLY AFFECT THOSE
AS WELL.
DELETE THINGS LIKE DROP BOX OR
OTHER THINGS THAT WAY.
AS MENTIONED THE ONLY WAY TO
MAKE YOUR BACK UP SECURE IS NOT
HAVE THEM ACCESSIBLE.
HAVE THEM ON THE SAME NETWORK
AND ABLING TO GO AROUND THE
NETWORK TO CROWS HIGHS OTHER

THINGS THAT COULD BE THE NEXT

TARGET.

>> SO WE HIT THE END OF OUR

SESSION.

I HAVE A COUPLE OF QUESTIONS

HERE FOR MODERATORS TO GET TO

LATER.

I WANT TO THANK VERY MUCH OUR

PANEL FOR THE INSIGHTS THIS

MORNING.

A GREAT KICK OFF FOR THE WORK

SHOP.

THANK YOU TO THEM.

[APPLAUSE]

;;;;Presentation by Office of Technology

>> WE'RE NEXT INVITED JOE

CALANDRINO AND ANTHONY MASI PRO

SENTING ORIGINAL RANSOM WARE

RESEARCH.

>> OVER THE PAST SUMMER WE HAD A

CROP OF FANTASTIC INTERNS

WORKING WITH US.

ONE OF THEM WAS ANTHONY.

ANTHONY HELPED US BETTER

UNDERSTAND THE RANSOMWARE THAET.

FOR THOSE WORKING WITH THE

GOVERNMENT IN THE ROOM, A PLUG,

ANTHONY IS A SCHOLARSHIP FOR

SERVICE RECIPIENT.

AFTER HIS DEGREE HE'S COMMITTED

TO WORK FOR THE GOVERNMENT FOR A

FEW YEARS.

I THINK THE QUALITY OF HIS WORK

SPEAKS FOR ITSELF.

THE PREVIOUS PANEL DID A GOOD

JOB OF INTRODUCING WHAT THE

RANSOMWARE THREAT IS OVER ALL.

TYPICALLY SOMETHING IS LOCKED

UP.

SOMEONE REQUESTS IF YOU GET

ACCESS TO THAT AGAIN YOU HAVE TO

GIVE THEM AN AMOUNT OF MONEY.

WHAT WE FOCUSED ON FOR OUR

PROJECT WAS THE MORE TRADITIONAL

FORM OF RANSOM.

THE DATA ON THE PC IS LOCKED UP.

IF YOU WANT ACCESS TO THAT ON

YOUR PERSONAL COMPUTER AGAIN YOU

PAY MONEY AND IT WILL BE

UNLOCKED AND YOU GET ACCESS TO

IT.

SO, HOW DO YOU GET IT.

ONCE AGAIN THE PREVIOUS PANEL

DELVED INTO IT QUITE A BIT.

THERE COULD BE A NUMBER OF WAYS.

ONE POSSIBLE VECTOR IS E-MAIL.

YOU MAY GET AN E-MAIL WITH A PDF

ATTACHED TO IT.

YOU THEN INFECT THE COMPUTER

OPENING IT UP.

ANOTHER IS DRIVE BY DOWNLOAD.

YOU VISIT A CERTAIN SITE.

THAT SITE IS PRO MICED AND IT

INFECTS YOUR COMPUTER WHEN YOU

VISIT IT OR THE AD NETWORK

SERVING ADS WITH A COMPROMISED

ADVERTISEMENT.

FROM THERE YOUR COMPUTER IS
INFECTED.
WE HAVE SPOKE TONE A NUMBER OF
PEOPLE VICTIM OF RANSOMWARE
SCAMS.
SOME JUST LOOKING FOR A LUNCH
ORDER.
WENT TO A LOCAL RESTAURANT SITE.
IT TURNS OUT THE WEB SERVER WAS
COMPROMISED AND AS A RESULT
COMPUTERS IN THE COMPANY WERE
COMPROMISED.
SO, WE'RE JUST GOING TO SHOW A
QUICK DEMO IN A MOMENT TO GIVE
YOU AN IDEA WHAT THIS LOOKS LIKE
WHEN YOUR COMPUTER IS INFECTED
IN PRACTICE.
IMAGINE YOU'RE DOING HR IN A
LARGE COMPANY.
YOU POST AID JOB.
YOU HAVE A BUNCH OF RESUMES.
WE DIDN'T GO THROUGH LOTS OF
TROUBLE SETTING THIS UP.

WE DIDN'T MAKE IT LOOK LIKE A

PDF FILE.

WE COULD OF SET UP SO IT DIDN'T

PROMPT TO YOU RUN THE RANSOMWARE

LIKE HERE.

THIS WILL GIVE YOU A ROUGH IDEA

WHAT IT LOOKS LIKE.

THERE WILL BE FLASHING LIKE

THIS.

IF YOU SUFFER FROM EPILEPSY OR

SOMETHING YOU MAY WANT TO DIVERT

YOUR EYES.

I WILL TELL YOU WHEN IT'S OVER.

PLAY THE VIDEO HERE.

THIS IS ONE VARY OF RANSOMWARE.

WE CLICKED ON THE PDF FILE.

WE HAVE OPENED IT UP AND AGREED

TO THE PROMPT COMING UP LIKE

MANY DO.

SUDDENLY THE COMPUTER REBOOTS.

LOOKS LIKE THE COMPUTER CRASHED.

WE GET A WARNING MESSAGE THE

DISK IS BEING CHECKED.

THIS MAY LOOK LEGITIMATE IF THE
COMPUTER WAS REBUTTING.
I WILL GIVE YOU THE HEADS UP
IT'S NOT CHECKING THE DISK
SOMETHING ELSE IS GOING ON.
WE WILL SEE WHAT IT IS IN A
MOMENT.
SO, LET'S HAVE A BRIEF PERIOD OF
AWKWARD SILENCE.
FINISHING IT'S TASK.
SUDDENLY WE HAVE FLASHING SKULLS
ON THE SCREEN AND THEN WE SEE A
MESSAGE TELLING US OUR COMPUTER
HAS BEEN COMPROMISED AND GIVING
US INSTRUCTIONS OF THE
REPAYMENT.
THIS COULD BE FAIRLY STARTLING
SOMEONE SEEING THIS
UNEXPECTEDLY.
SO, OUR GOAL WITH THE SUMMER
PROJECT WE HAD ANTHONY WORKING
ON WAS BETTER UNDERSTAND THE
BEHAVIOR OF RANSOMWARE AND THE

EXPERIENCE OF VICTIMS OF

RANSOMWARE.

I WILL HAND THIS OFF TO ANTHONY

ON HOW HE DID THAT.

>> OKAY.

COOL.

OKAY.

SO THE METHODOLOGY OF THE

PROJECT I FIRST OBTAINED MY

SAMPLES.

INFECTED VIRTUAL MACHINES AND

SAW THE RESULTS.

WITH THAT COMPLETE I WENT ONTO

COMMUNICATE WITH THE AUTHORS OF

RANSOMWARE.

I CHOSE THE SAMPLES BRUISING

THROUGH THE MAL WARE -- USING

FOR RANSOMWARE TAGGED SAMPLES.

THEY ARE FROM A THREE MONTH

PERIOD THIS SPRING TO EARLY

SUMMER.

SO, I SET UP A VIRTUAL MACHINE

WHICH FOR THE PURPOSE OF THIS

PROJECT SERVED AS A SIMULATION
OF A PERSONAL COMPUTER RUNNING
WINDOWS 7.
I EXECUTED EACH SAMPLE ON THIS
MACHINE INCLUDING CANARY FILES
OR DUMMY FILES THAT REPRESENTED
ABOUT 300 DIFFERENT COMMON FILE
TYPES.
THE PURPOSE WAS TO SEE THE FILE
TYPES THE RANSOMWARE TARGETED
AND WHETHER IT WAS SELECTIVE IN
THE ENCRYPTION.
DURING THE PROCESS OF THE
RESEARCH I HAD FOUR SEPARATE
CONFIGURATION FOR EACH SAMPLE.
I SET THE WINDOWS LOCAL TO
EITHER INDAN, JAPANESE, RUSSIAN
OR THE AMERICAN LOCAL.
I CHOSE THESE DUE TO THESE BEING
FOUR OF THE MOST COMMON NATIONS
AFFECTED BY RANSOMWARE.
AT THE SAME TIME GEOGRAPHIC I
CANNILY AND ECONOMICALLY

DIVERSE.

IT'S FARE TO NOTE THE IP ADDRESS

OF THE MACHINE REMAINED THE

SAME.

IT'S POSSIBLE THE AUTHORS WERE

DETERMINED ALL OF THE INFECTIONS

WERE OCCURRING FROM THE SAME

PLACE.

SO MY SUCCESS RATE WAS ABOUT

60 PERCENT.

IT WASN'T A HUNDRED PERCENT.

THERE IS A SHORT SAMPLE LIFE

SPAN.

THE INFRASTRUCTURE IS QUICK TO

GO DOWN DUE TO LAW ENFORCEMENT

OR JUST THE AUTHORS ATTEMPTING

TO REMAIN UNDER THE RADAR

SWITCHING DEMAND AND CONTROL

SERVERS OR DOMAIN NAMES RAPIDLY.

ANOTHER POSSIBLE MAYBE

ANTI-ANALYSIS TECHNIQUES.

I WOULD LIKE TO NOTE THE

STATISTIC UNDERSTAND REPRESENTED

HERE ARE REPRESENTATIVE OF THOSE
IN MY RESEARCH AND SHOULDN'T BE
TAKEN AS INDICATIVE OF THE
SUCCESS RATE IN THE WILD.
HERE IS FIRST EXAMPLE OF ONE I
CAME ACROSS AS SEEN PREVIOUSLY.
THIS IS CALLED JIGSAW.
YOU CAN SEE A TIMER ON THE
SCREEN.
THE AUTHOR LIKES TO FRAME THIS
AS A GAME.
INTRODUCES EXPONENTIAL GROWTH.
AN HOUR YOU LOSE TEN, ANOTHER
HOUR YOU LOSE MORE AND SO ON
UNTIL YOU PAY THE RANSOM.
THERE IS AN ARBITRARY TIME SET
IF YOU DON'T PAY THE FILES ARE
GONE FOREVER.
I DIDN'T TEST IF THAT WAS TRUE.
YOU CAN SEE AT THE BOTTOM
BLOCKED OUT BY THE RED BAR A
BITWALLET ADDRESS.
THAT WAS THE FORM OF PAYMENT FOR

THIS VARIANT.

IT WAS ALL PRESENTED TO THE USER

THROUGH THIS WINDOW.

HERE IS ANOTHER VARIANT KNOWN AS

CRIES CRISIS.

THIS VARIED SLIGHTLY FROM THE

PREVIOUS INFECTION I SHOWED YOU.

YOU CAN SEE THIS CHANGED YOUR

DESK TOP BACKGROUND.

IT LEAVES YOU A NOTE THAT IS NOT

IN PERFECT ENGLISH.

A SCARED TACTIC OF A MAN IN CAMO

WITH A LARGE GUN.

IT LEAVES BEHIND AN E-MAIL

ADDRESS AS WELL.

FOR FURTHER INFORMATION

REGARDING PAYMENT OF THE RANSOM

OR HOW MUCH IT COST YOU HAVE TO

REACH OUT TO THE E-MAIL.

SO, A THIRD, A THIRD VARIANT

THIS.

IS ON LOCK 92.

THIS WAS WRITTEN IN RUSSIAN,

RANSOM NOTE.

AFTER TRANSLATING THIS NOTE IT

KIND OF FOLLOWS THE SAME FORMAT

AS THE TWO PREVIOUS RANSOM

NOTES.

IT IS SAYING YOUR FILES ARE

ENCRYPTED.

CONTACT ME OR VISIT THIS WEBPAGE

FOR PAYMENT.

A WEBPAGE IS INCLUDED AND AN

E-MAIL FOR CUSTOMER SUPPORT.

SO, AS YOU CAN SEE THE

RANSOMWARE AUTHORS USE DIFFERENT

PRESSURE TACTICS TO GET YOU TO

PAY.

FILE DELETION THREATS.

ONE SAMPLE DIDN'T ENCRYPT

ANYTHING.

IT CLAIMED TO HIDE YOUR

TPAOEULDZ AND AFTER PAYMENT YOU

WOULD GET THE FILES BACK.

THAT WOULDN'T HAPPEN.

YOU PAID $500 AND THE FILES WERE

GONE REGARDLESS IF YOU PAID OR

NOT.

THERE IS THE IN CRESS IN PRICE

TACTIC YOU SAW WITH THE JIGSAW

SCAM APPROXIMATELY.

A COMMON WAS THREE DAYS.

AFTER THREE DAYS THE PRICE GOES

UP.

A SHORT ACTION WINDOW PREVENTS

YOU FROM TALKING TO A THIRD

PARTY OR ANY RESEARCH.

YOU PREFER TO GET YOUR FILES

BACK BEFORE ANYTHING HAPPENS TO

THEM.

THE FRIGHTENING USER EXPERIENCE.

THE MAN IN THE CAMO WITH THE

GUN, A CHARACTER TPRER A HORROR

MOVIE AND A BUNCH OF EXAMPLES.

ONE SERVER SORT OF PWHRAEURZ A

MESSAGE TO YOU FROM THE

COMPUTER.

YOUR COMPUTER PLAYS AN AUTOMATED

MESSAGE SAYING YOUR FILES ARE EN

CRIPPED.

THIS ARE AGGRESSIVE DELETION

TACTICS.

WE HAVE SEEN REPORTS OF

EXFILTRATION.

DURING MIER ARE SEARCH I DIDN'T

OBSERVE IF DATA WAS EXFILL TRAIT

TODAY THIRD PARTY SERVER.

SO, THIS IS MY SUCCESS RATE BY

COUNTRY.

AS YOU CAN SEE ALL OF THE

SAMPLES RAN WHEN IT WAS SET TO

INDIA, JAPANESE AND U.S.

ONLY 90 PERCENT WHEN SET TO THE

RUSSIAN LOCAL.

IN THIS CASE THE PROCESS WOULD

START.

AFTER A COUPLE OF SECONDS IT

WOULD HALT AND IDLE OR CLOSE

ITSELF.

IT'S FARE TO NOTE THE ORIGIN OF

THE SAMPLES WERE A ENGLISH

SPEAKING MAL WARE RESOS TORY REPOSITORY.

THIS IS THE LANGUAGE.

80 PERCENT IN ENGLISH.

23 PERCENT IN RUSH YAWN.

RUSSIAN AND 3 INITALIAN.

THAT'S MORE THAN A HUNDRED

PERCENT.

SOME HAD ENGLISH AND RUSSIAN.

SO, OF THE 30 SAMPLES WE

OBSERVED ENCRYPTING FILES ON THE

VIRTUAL MACHINE 21 ENCRYPTED OUR

CAN AIRY FOLDER.

SOME SKIPPED THE FOLDER.

SOME BLOCKED ACCESS TO THE PC.

SOME SIMPLY TKHROETED FILES

INTENTIONALLY OR DUE TO JUST

SHOTLY CODED.

ENCRYPTION MAY OF OCCURRED IN

OTHER POINTS OF THE SYSTEM.

FOR THE PURPOSE OF THE ACADEMIC

STUDY WE FOCUSED ON THE CAN

ARROW FOLDER.

WE DISREGARDED SAMPLES

ENCRYPTING EVERYTHING BUT THAT.

SO, HERE YOU CAN SEE A YAH OF
THE FILE TYPES ENCRYPTED.
TOWARDS THE LEFT OF THE GRAPH
YOU WILL SEE A LOT OF FILE TYPES
THAT ARE FAMILIAR TO YOU.
CASUAL COMPUTER USE.
I BELIEVE ALL OF THE SAMPLES
ENCRYPTED MICROSOFT WORD
DOCUMENTS J PEG IMAGES LIKE A
DIGITAL CAMERA OR CELLPHONE,
GOING FURTHER DOWN THE LIST YOU
MAY SEE THE PDF PORTABLE
DOCUMENT FORMAT, DATABASES, FILE
TYPES THAT ARE USED BY I AM
STATION SOFTWARE.
SINCE I HAD ABOUT 300 SAMPLES,
THROW HUNDRED DIFFERENT FILE
EXTENSIONS IT'S FARE TO NOTE THE
DIFFERENT CATEGORIES OF FILES
ENCRYPTED BY THE RANSOMWARE.
YOU CAN SEE A COMPUTER CODE,
MULTI MEDIA, SPECIFIC FILES
RELATED TO ENCRYPTION, VIRTUAL

MACHINE RELATED FILES.

VIRTUAL MACHINE DISK FILES.

VIRTUAL CARDS, TAX INFORMATION

SO IT'S INTERESTING TO NOTE THAT

THE RANSOMWARE AUTHORS MAY GO

AFTER THESE CATEGORIES DO TO THE

FACT THEY'RE HARD TO REPLACE.

YOU CAN'T PULL MORE IMAGES OFF

OF THE SMART PHONE.

THINGS THAT ARE VALUABLE TO YOU.

THAT MAYBE THE REASON BEHIND THE

FILE FORMATS CHOSEN.

THE AVERAGE RANSOM AMOUNT

INITIALLY WAS ABOUT $570.

WHICH -- IS FAIRLY LARGE SUM OF

MONEY ON THE PC.

WE SAW A MINIMUM AMOUNT -- UP TO

$3300 IN ONE CASE.

NOW IF YOU WERE TO WAIT FOR AN

ARBITRARY TIME PERIOD.

LIKE THE EXAMPLE BEFORE WAS

ABOUT THREE DAYS.

THE RANDOM WOULD GENERALLY GO

UP.

THE AVERAGE IN THAT CASE WENT UP

TO ABOUT $715.

WE SUE THE MEDIAN AMOUNT RISE TO

$436.

WHILE THE MINIMAX WERE ROUGHLY

UNCHANGED.

SO THERE ARE A COUPLE OF OTHER

NOTE WORK WORTHY THINGS I

OBSERVED DURING THE RESEARCH.

THE VARIANCE, ACCESS REGISTERING

KEY TO E-MAIL CLIENTS

CREDENTIALS, ACTIVITIES OF KEY

LOGGING, COLLECTION OF PRIVATE

INFORMATION FROM THE BROWSER AND

BROWSER HISTORY, AND BOOK MARKS

AND GEO LOCATION EXAMINATION.

SOME SOUGHT THE EXTERNAL IP

ADDRESS AND WHERE THE PC IS

LOCATED IN THE WORLD.

SO, DURING MY ANALYSIS I CAME

ACROSS A BUNCH OF URLs LEFT

BEHIND A SPECIFIC SAMPLE.

WHEN LOOKING TO EXAMINE THE
CANNING CONTROL SERVES WHERE THE
DECRYPTER WAS LOCATED I NOTICED
ONE WAS WITH A SMALL BUSINESS.
A MOM AND POP STORE IN THE
UNITED STATES.
ALONG WITH PHEBE -- OF OTEP WE
WERE ABLE TO FIND A COUPLE OF
VARIABLES IN THE QUEARY STRING
AND RECOVER WINE AIR HE'S THAT
WERE INDICATIVE OF DISTRIBUTING
RANSOMWARE AND THOSE OF PREUF
LEMED.
ANOTHER FORM OF MAL WARE
UNRELATED TO THE MAL WARE.
RUED FOR DATA AND KEY LOGGING
AND A PHP -- I SAID THAT.
WE WERE ABLE TO, WE WERE ABLE TO
CONTACT THE OWNER OF THIS
WEBSITE.
INFORM THEM THE WEB WAGE WAS DIB
TRIBUTING THIS WHAT WAS
INTERESTING IS THEY APPEARED TO

BE COMPROMISED THROUGH THE WEB

STORE.

THEY WERE UNAWARE WHEN ACCESSING

THEIR WEBSITE.

THE RANSOMWARE, DESTRICTER AND

OTHER BAD FILES WERE LOCATED IN

A DIRECTORY TUCKED AWAY.

ONE ACCESSED VIA URL PROVIDED IF

YOU WERE INFECTED WITH THE

RANSOMWARE.

SO THE WEBSITE WAS SHORTLY

DECOMMISSIONED.

>> OKAY.

RECALL EARLIER THE RANSOMWARE

PROVIDED US WITH E-MAILS FOR THE

AUTHORS AND THE PEOPLE BEHIND

THE RANSOMWARE AND OTHER THINGS.

WE WANTED TO REACH OUT AND SEE

WHAT THE ATTRACTIONS MIGHT BE

BETWEEN THE VICTIMS OF

RANSOMWARE AND THE PEOPLE BEHIND

IT.

THE IDEA WAS TO GET AN IDEA OF

THE RANSOM PHAOUPBTSZ YOU MAY
GET AND WHETHER YOU COULD
NEGOTIATE AND GENERALLY WHAT THE
EXPERIENCE MIGHT BE LIKE.
WE WANTED TO REPLICATE THE BASIC
PROCEDURES.
WE DEVELOPED SCRIPTS INTEND TODD
TARGET A INDAN CASE, U.S. CASE,
JAPANESE CASE AND A RUSSIAN
CASE.
WE USED ENGLISH LANGUAGE WITH
INDAN IDIOMS FOR THE INDAN CASE.
FOR THE U.S. WE USED U.S.
IDIOMS.
FOR JAPANESE WE USED JAPANESE
LANGUAGE.
FOR THE RUSSIAN CASE WE USED
RUSSIAN LANGUAGE.
WE LAY LIMITED NUMBER OF SAMPLES
FOR THIS.
IF YOU CONTACT ONE IN A LANGUAGE
AND SEND THEM A NOTE IN A
DIFFERENT LANGUAGE THEY MAY

CATCH ON.

WE WANT TO RANDOMIZE THE ORE +*D

ORDER FOR INITIAL RESULTS.

THESE ARE NOT SIGNIFICANT BUT

HINTS OF WHAT TO OBSERVE IN

PRACTICE.

WE DO THE EQUIVALENT OF FLIPPING

A COIN TO FIGURE THE LADIES AND

GENTLEMENNAGE TO REACH OUT

FIRST.

THEN RANDOMIZE IT AFTER THAT.

WITH THE GOAL OF THE E-MAIL

ADDRESSES WE WOULD GET DIVERSITY

IN TERMS OF THE LANGUAGE OR

COUNTRY THAT WE WERE USING TO

REACH OUT TO EACH ONE.

AND ALSO IT'S WORTH NOTING FOR

EACH ONE WE USED A WEB MAIL

ADDRESS THAT WOULD OF BEEN

POPULAR IN THE CORRESPONDING

COUNTRY.

WE HAD 13 SAM P-LDZ OVER ALL TO

REACH OUT.

OUT OF THOSE TEN WERE

FUNCTIONAL.

THREE WERE NOT FUNCTIONAL.

IT RAISES A QUESTION WHAT

HAPPENS IF YOUR COMPUTER IS

INFECTED.

YOU ATTEMPT TO REACH OUT AND IT

BOUNCES BACK.

WHAT DO YOU DO FROM THERE IF YOU

ARE PAYING THE RANSOM.

IT'S A PRETTY DIFFICULT

POSITION.

SO WE REACHED OUT TO ALL TEN

THAT DIDN'T BOUNCE BACK.

SIX OF THEM YIELDED RESPONSES

FOR AT LEAST ONE OF THE FOUR

COUNTRY CASES I MENTIONED

EARLIER.

VIRTUALLY ALL RESPONDED TO THE

DIFFERENT CASES WITH THREE

EXCEPTIONS.

FOR ONE CASE WE DIDN'T GET A

RESPONSE FOR THE INDAN CASE.

AND TWO FOR THE JAPANESE TEST

CASES.

NOW THERE ARE SPOT LANGUAGES

SKEWED TOWARDS ENGLISH.

IT'S WORTH NOTING FOR HALF OF

THE CASES HALF OF THE

COMMUNICATION WAS IN ENGLISH.

THE ORIGIN WAS AN ENGLISH SITE.

THIS IS NOT TOTALLY SURPRISING

TO US BECAUSE OF THE POPULARITY

OF ENGLISH.

THIS IS THE RESPONSE EXAMPLE WE

SAW BACK.

THE PERSON DESCRIBED WHAT THEY

HAVE BUN, A FREE SECURITY SCAN

ON THE COMPUTER.

COMPUTER SCANS COST TENS OF

THOUSANDS OF DOLLARS IT'S ALL

FOR FREE.

NOW THEY CAN STORE ABOUT 2.5 BIT

COINS MAY INCREASE TO P BIT

COINS.

THAT'S BETWEEN 1500 TO $1800.

SO THEY ARE PROVIDING THESE

PEOPLE WITH A GREAT SERVICE.

NOW HERE IS AN EXAMPLE OF AN

ANECDOTE AL NEGOTIATION.

I CHOSE THIS IT'S NOT

REPRESENTATIVE OF ALL THE CASES

WE GOT RESPONSES FOR THE

DIFFERENT LANGUAGES AND FOR,

ALSO WE PROCEED PRO +*E SEEDD WITH

A MEASURE OF NEGOTIATION WITH

THEM MUCH BEFORE WE SKWRUPL TO A

CONCLUSION THIS IS ILL STRAY

TIFF OF ALL CASES I WILL TKHREFL

INTO THE SPECIFICS.

FOR EACH CASE WE REACHED OUT.

THE INDAN CASE, U.S. AND

JAPANESE CASE WE GOT A QUOTE OF

$1200 INITIALLY.

FOR THE RUSSIAN CASE WE GOT A

QUOTE OF .4 BIT COINS JUST UNDER

250 TKHRAORZ.

WE PROCEEDED TO NEGOTIATE DOWN

THE PRICES FOR EACH CASE.

FOR THE INDAN CASE AND U.S. CASE
WE GOT THE AMOUNT BELOW $900.
FOR THE JAPANESE CASE SLIGHTLY
ABOVE $900.
WE NOTICED THIS FOR A COUPLE OF
EXAMPLE CASES.
THE JAPANESE CASE WAS SLIGHTLY
ABOVE THE OTHER CASES.
THIS COULD BE VARIOUS REASONS
THAT MAY OCCUR.
MAYBE THAT JAPANESE LANGUAGE IS
LESS GEOGRAPHICKY DISTRIBUTED
AND TIE TODAY HIGHER LEVEL OF
GDT.
WE DON'T HAVE THE DATA TO BACK
THAT UP.
FOR THE RUSSIAN CASE WE WERE
ABLE TO NEGOTIATE TO DOWN BELOW
$200.
NOW FOR THREE SAMPLES OR THREE
OVER ALL WE NEGOTIATED DOWN THE
AMOUNT.
FOR THREE OUT OF THE SIX WE

NEGOTIATED DOWN.

SINCE WE DIDN'T PAY THE RAN

SOPLZ WE DON'T KNOW IF PEOPLE

HELD TO THE AMOUNTS THEY SAID.

THIS IS AN EARLY INDICATION IT

MIGHT BE WORTHWHILE TO NEGOTIATE

DOWN IF YOU IN FEND TO PAY THE

RANSOM.

IF YOU SHOULD OR SHOULDN'T IS A

DIFFERENT QUESTION.

IT'S WORTH NOTING FOR THE

RUSSIAN CASE, THE JAPANESE CASE

WAS A TREND WE SAW ACROSS

SAMPLES.

IN MANY CASE THE RUSSIAN WAS

SIMILAR ACROSS THE SAMPLES WE.

THIS HINTS DIFFERENS BASED ON

LOCAL.

IN TERMS OF FUTURE WORK ONE AREA

YOU MAY LOOK AT IS DEEPER

ANALYSIS AND POSSIBLE REVERSE

ENGINEERING TO FIGURE OUT WHAT

IS HAPPENING IN THE RANSOMWARE.

ANTHONY HINTED AT WHAT WE HAVE

SEEN.

ONE COULD DIVE DEEPER AND SEE

WHAT THE CODE IS ACTUALLY DOING

IN PRACTICE.

ALSO YOU CAN DO MORE FORENSIC

ANALYSIS.

WE NOTICED SOME RANSOMWARE

SUPERFICIALLY LOOKED SIMILAR.

BASED ON RANSOMWARE AS A SERVICE

IT'S POSSIBLE THEY'RE DEVELOPING

EFFECTIVELY THESE PIECES.

IT LOOKS LIKELY DIFFERENT BUT

DEVELOPED BY THE SAME GROUP OF

PEOPLE PERFORMING SIMILARLY.

MORE GENERALLY YOU MAY EXPLORE

THIS IS A SERVICE

INFRASTRUCTURE.

IT MAYBE WORTHWHILE LOOKING INTO

EMERGING THREATS.

GEORGIA GAVE GREAT EXAMPLES.

TARGETING MOBILE DEVICES AND

THERMOSTATS.

WE HAVE SEEN THINGS LIKE ANDROID
TVs CAN BE LOCKED DOWN LIKE
ANDROID PHONES.
SO, IN CONCLUSION WE SAW RANSOM
AMOUNTS FROM $15 TO JUST UNDER
$3300.
THE EXAMPLE PIECE OF RANSOMWARE
WE TESTED.
WE NOTICED DWIGHT A BIT OF
ENCRYPTION OF HIGH VALUE DATA
AND HIGH PRESSURE TACTICS TO GET
TO YOU PAY AND PAY QUICKLY.
WE SA +*U HINTS OF HOW THESE PIECE
OF RANSOMWARE OPERATE AND YOUR
INTERACTIONS BEHIND THE RAM SON
WARE.
OVER ALL THIS CAN BE A CHALLENGE
TO AVOID AND MITIGATE.
THINGS LIKE THE RESTAURANT CASE
YOU MAY VISIT A WEBSITE AND GET
INFECTED.
OVER ALL THIS IS AN EVOLVING
FUTURE THREAT.

SO WITH THAT I WILL LET GUILTY

TO YOUR BREAK.

THANK YOU SO MUCH.

[APPLAUSE]

>> SHOCKINGLY WE'RE A AHEAD OF

SCHEDULE.

WE ARE TAKING A QUICK BREAK.

THE NEXT PANEL WILL START AT

3:00 P.M.