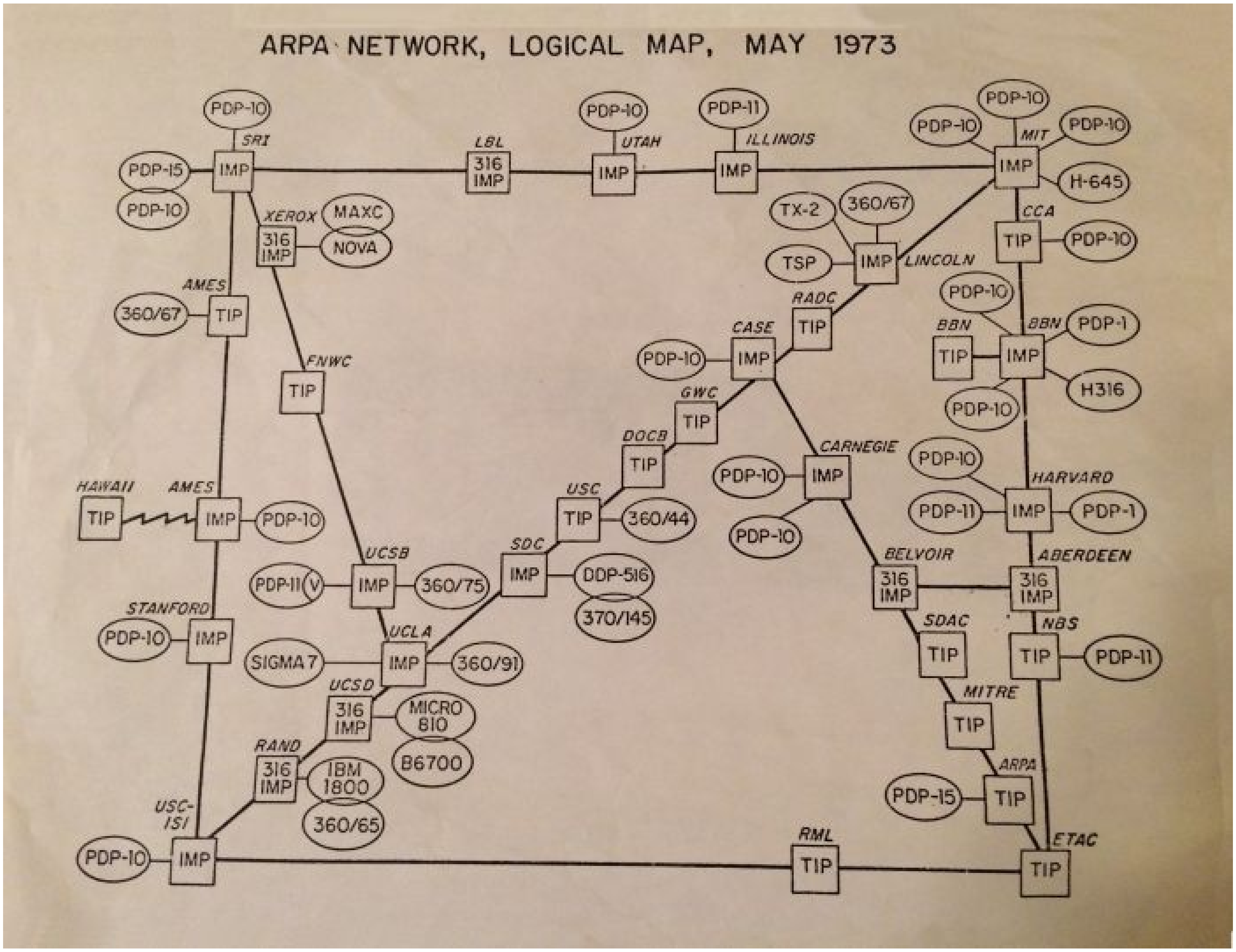
Security Now! #590 - 12-13-16

Q&A #245

This week on Security Now!

- Ticket-buying bots get their hand slapped (do they have hands?)
- A truly nasty new addition to encrypting ransomware operation.
- A really dumb old problem returns to many recent Netgear routers.
- Yahoo!'s too pleased with their bug bounty program.
- Steganometric advertising malware went undetected for two years.
- uBlock Origin readies for a big new platform.
- What exactly is the BitDefender "BOX"? We wish we knew!
- VeraCrypt was audited... next up is OpenVPN! (Yay!)
- Steve's found a new relaxing and endless puzzler, And... questions from our listeners!



https://media.grc.com/The-Internet-Circa-1973.jpg

Security News

Congress passes "BOTS Act" to ban ticket-buying bots
BOTS: Better Online Ticket Sales
Bill S.3183 - BOTS Act of 2016
https://www.congress.gov/bill/114th-congress/senate-bill/3183
Better Online Ticket Sales Act of 2016 or the BOTS Act of 2016

(Sec. 2) This bill prohibits the circumvention of a security measure, access control system, or other technological measure on an Internet website or online service of a ticket issuer that is used to enforce posted event ticket purchasing limits or to maintain the integrity of posted online ticket purchasing order rules for a public event with an attendance capacity exceeding 200 persons.

The bill also prohibits the sale of or offers to sell an event ticket in interstate commerce obtained through such a circumvention violation if the seller participated in, had the ability to control, or should have known about the violation.

It shall not be unlawful, however, to create or use software or systems to: (1) investigate, or further the enforcement or defense of, alleged violations; or (2) identify and analyze flaws and vulnerabilities of security measures to advance the state of knowledge in the field of computer system security or to assist in the development of computer security products.

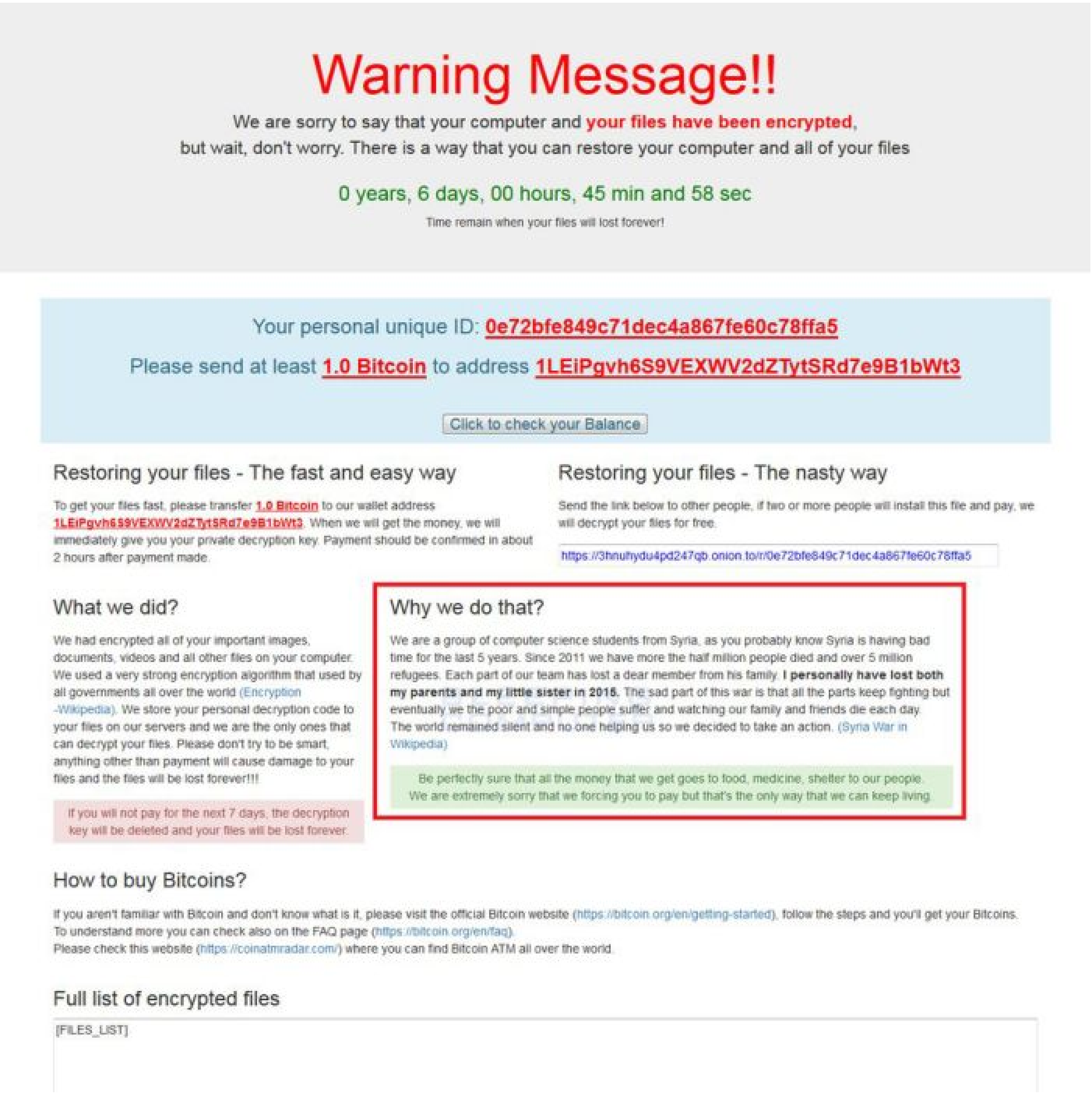
Violations shall be treated as unfair or deceptive acts or practices under the Federal Trade Commission Act.

The bill provides authority to the Federal Trade Commission and states to enforce against such violations.

Introducing "Popcorn Time", the latest twist in file encrypting malware:

- When a victim's machine is infected they have a choice:
    - Either pay one bitcoin -- currently ~$780 --
    - -OR- successfully infect two other people, who then pay up, by arranging to cause them to invoke the specially tagged "credit link" provided.
- And, as if these guys were not cretinous enough, they then proceed to claim that they are Syrian and that the proceeds from this extortion "will be used for food, medicine, and shelter to those in need."
- "We are extremely sorry that we are forcing you to pay but that's the only way that we can keep living."
- And, just in case you still thought they might be good guys, reverse engineering of the code appears to indicate that four wrong entries of the key will trigger permanent deletion of the still-encrypted files.

- Warning Message:
    - https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/



Warning Message!!

We are sorry to say that your computer and **your files have been encrypted**,
but wait, don't worry. There is a way that you can restore your computer and all of your files

0 years, 6 days, 00 hours, 45 min and 58 sec

Time remain when your files will lost forever!

Your personal unique ID: **0e72bfe849c71dec4a867fe60c78ffa5**

Please send at least **1.0 Bitcoin** to address **1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3**

Restoring your files - The fast and easy way

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5

What we did?

We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world (Encryption -Wikipedia). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!

If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.

Why we do that?

We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more the half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. **I personally have lost both my parents and my little sister in 2016.** The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. (Syria War in Wikipedia)

Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people.
We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.

How to buy Bitcoins?

If you aren't familiar with Bitcoin and don't know what is it, please visit the official Bitcoin website (https://bitcoin.org/en/getting-started), follow the steps and you'll get your Bitcoins.
To understand more you can check also on the FAQ page (https://bitcoin.org/en/faq).
Please check this website (https://coinatmradar.com/) where you can find Bitcoin ATM all over the world.

Full list of encrypted files

[FILES_LIST]

A dumb "blast from the past" mistake found to affect many models of Netgear routers.

Affected models:

- R6250, R6400 (AC1750), R6700, R7000 Nighthawk (AC1900, AC2300),
- R7100LG, R7300, R7500 Nighthawk X4 (AC2350), R7800 Nighthawk X4S(AC2600),
- R7900, R8000 Nighthawk (AC3200), R8500 Nighthawk X8 (AC5300), R9000,
- Nighthawk X10 (AD7200)

Unbelievable….

- **http://<local router LAN_IP>/cgi-bin/;COMMAND**

CERT advisory issued

- https://www.kb.cert.org/vuls/id/582384
- Vulnerability Note VU#582384
- Multiple Netgear routers are vulnerable to arbitrary command injection
- <quote> Improper Neutralization of Special Elements used in a Command ('Command Injection')
- https://www.exploit-db.com/exploits/40889/

- Workaround: Disable the router's web server... using the exploit! <g>
  - http://<router_IP>/cgi-bin/;killall$IFS'httpd'

Check for vulnerability:

- **http://[router-address]/cgi-bin/;uname$IFS-a**

Michael Horowitz, on his Denfensive Computing blog at ComputerWorld, suggests:

- **http://1.2.3.4/cgi-bin/;reboot**

Bas' Blog

- A temporary fix for CERT VU#582384 vulnerability for various Netgear routers (including R6400, R7000, R8000 and similar)
- http://www.sj-vs.net/a-temporary-fix-for-cert-vu582384-cwe-77-on-netgear-r7000-and-r6400-routers/

Netgear acknowledges the problem

- http://kb.netgear.com/000036386/CVE-2016-582384
- Beta firmware now available for: R6400, R7000, R8000

I called this a "blast from the past" problem, since it feels like the sorts of problems we had around the turn of the century when it was first dawning upon us that not everyone was a good guy... and that bad guys could get up to a lot of mischief with the inherently trusting systems we had back then.

Yahoo!'s too-successful Bug Bounty Program

- Speaking of "classic" web bugs, Yahoo! just paid $10,000 to a Finnish security researcher who found and responsibly reported a means for anyone to accesses anyone else's Yahoo! mailbox simply be sending them a specially crafted eMail.

- Yahoo! had a Cross-Site Scripting (XSS) bug.

- The security researcher discovered that an attacker could sneak malicious JavaScript code past Yahoo Mail’s filters by abusing the way Yahoo Mail displays links to sites such as YouTube. All that was necessary was to embed JavaScript within a specially-crafted email containing a YouTube video link.

- No action was required on the recipient's end. Nothing to click... just viewing the eMail would xecute the embedded JavaScript in the trusted context of the user
- Researcher's Blog Posting: https://klikki.fi/adv/yahoo2.html

- A Yahoo spokesperson said that the company ”has developed one of the largest and most successful bug bounty programs in the industry.” <quote> "We've paid out more than $2 million in bounties, resolved more than 3,000 security bugs and maintain a 'hackership' of more than 2,000 researchers, some of whom make careers out of it," the spokesperson's email statement read.

Practical Applied Steganometry

- Malware infects computers by hiding in browser ad images
- The "Steganos" exploit kit went undetected for two years by avoiding security analysts' computers.
- ESet researchers found this very tricky bug.
- It's been operating stealthily for the last two years and specifically targeting corporate payment and banking services.
- Innocuous JavaScript was able to extract additional code from the TRASPARENCY channel of image.
- https://www.engadget.com/2016/12/08/malware-infects-computers-by-hiding-in-browser-ad-gifs/

uBlock Origin is previewing for the Edge Browser

- https://www.neowin.net/news/ublock-origin-makes-its-way-to-microsoft-edge-in-preview-form
- https://www.microsoft.com/en-us/store/p/ublock-origin/9nblggh444l4

NYT: "Worried About the Privacy of Your Messages? Download Signal"

- http://www.nytimes.com/2016/12/07/technology/personaltech/worried-about-the-privacy-of-your-messages-download-signal.html

- <quote> BY the time you finish reading this column, you would be foolish not to download the messaging app Signal onto your smartphone and computer.

  The free encrypted messaging service has won the acclaim of security researchers and privacy advocates, including Edward J. Snowden. All have said that Signal goes above and beyond other chat tools in keeping electronic communications private.

  Signal is one of many encrypted messaging services, but it stands out for its uncompromising security and ease of use. The chat service retains virtually no information from users, including messages and address books, on its servers. What’s more, messages remain encrypted when passing through Signal’s servers, meaning that the app’s creators can’t read them.

- We know that FoaceBook’s WhatsApp also adopted the Signal protocol, which we have previously discussed at some length… but sophisticate users are encouraged to use Signal, and to DEFINITELY activate the “notify if fingerprint changes” option.

The BitDefender "BOX"

- http://www.bitdefender.com/box/
- "Agents" apparently must be installed on every device
- Windows, Macs, iOS & Android
- But, but, but... there's no technical explanation.
- We know the "CuJo" was junk since it was unable to see into HTTPS comms.

VeraCrypt was audited. Next up is OpenVPN!

- OSTIF Official (@OSTIFofficial) / 12/10/16, 12:30 AM
  @SecurityNow @leolaporte @SGgrc
  You guys did a great piece on our VeraCrypt audit.
  We are at it again with @OpenVPN
  https://ostif.org/ostif-is-beginning-a-fundraiser-for-openvpn-lets-get-it-audited/

- This effort was launched exactly three weeks ago, on November 22nd.
- OpenVPN v2.4 is in beta… preparing for the first major release in years.

- Leading the effort, the groups that have made significant contributions to the cause:
  - iPredator has contributed 10 BTC or about $7700
  - OpenVPN Technologies Inc. has contributed $5000
  - Perfect Privacy has contributed $3500
  - nVpn.net has contributed $2650
  - ExpressVPN has contributed $2500
  - SmartDNSProxy has contributed $2500
  - iVPN has contributed $2100
  - SecureVPN.to has contributed $1500
  - VPN.ac has contributed $1500
  - GetFlix has contributed $1350
  - TrickByte has contributed $1150
  - VikingVPN has contributed $1000, making their total contribution to OSTIF $2000.
  - NordVPN has contributed $1000

- Also contributing to the effort:
  - FatDisco has contributed $650
  - BestSmartDNS has contributed $600
  - Windscribe has contributed $500
  - Celo.net has contributed $400
  - ThatOnePrivacySite has contributed $200. They have also agreed to add a field to their famous VPN Comparison Chart showing which VPN services contribute back to the privacy community. (under activism – gives back to privacy causes)
  - VPNcompare.co.uk has contributed $201
  - BestVPN has contributed $300 and plans to write an article about the fundraiser, helping us reach out the privacy community!
  - InvizBox has contributed $100

- Beginning today, we are going to attempt to contact every commercial VPN provider in the world about supporting the effort.

- The OSTIF group's goal is to raise $71K… they are about half way there.

- **THEN…** Headline: "Private Internet Access funds OpenVPN 2.4 audit by noted cryptographer Dr. Matthew Green"
    - https://www.privateinternetaccess.com/blog/2016/12/private-internet-access-funds-openvpn-2-4-audit-noted-cryptographer-dr-matthew-green/

- The OSTIF guys are annoyed, since they report that they had previously reached out to the "Private Internet Access" (PIA) folks without success… and only after that PIA announced their intent to do their own. So long as PIA doesn't prevent OSTIF, fine.

Miscellany

■ **Square it!** (Unicode 'block' char in name... much like the infinity symbol in Infinite Loop.)

- From the folks who brought us Infinite Loop.
- iOS & Android
- FREE with between-level ads -- $1 to remove'em.
- Excellent, relaxing, just right, I think.
- Download links for "¦ Square it!" Relaxing Puzzle:
    - iOS: https://itunes.apple.com/us/app/square-it!/id1160380201
    - Android: https://play.google.com/store/apps/details?id=com.infinitygames.squareit

Looks like it's "Thumb Out"

SpinRite

Justin Alcorn (@JaBbA64)
@SGgrc Spinrite L4, 500G Drive. 350M ecc corrected. 21M seek errors.
Throw it away, or did we just fix it?