THE PACKET

THE UNIVERSITY OF ARIZONA

FALL

DECEMBER 2020

THE UNIVERSITY OF ARIZONA THE PACKET DECEMBER 2020

IN THIS ISSUE

--- BEGIN MESSAGE ---

Welcome to the **DECEMBER** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and I hope everyone enjoyed our previous Thanksgiving break and our upcoming end of the semester. The global community has almost been dealing with COVID-19 for an entire year and within this short time there have been many changes to the cyber security community. Working from home is almost the industry standard across the board and in many other industries they are having to adjust as this reality sets in. Many organizations were unprepared for this major shift and the consequences to cybersecurity are still being realized. In the United States we just completed a presidential election where many chose to utilize mail in voting for the first time and while every system takes time to adjust, this appears to be a successful method in the year 2020. Ransomware events appear to be more common and many organizations are realizing that once infected the data that has been encrypted is also very likely going to be released for additional payments and exploitation. Every industry must further adapt, and this means more reliance on cybersecurity professionals. Once you graduate from your program you will find many organizations who realize for the first time that they need to take cybersecurity seriously and you will be on the front lines of many networks that have not been securely maintained but made to be efficiently ran for business and revenue generation. The gold standard for how organizations need to operate is adjusting and many are taking note and will rely on you and your new skill sets. -- Good Luck --

--- END MESSAGE ---

CYBER CLASSIFIED BY: PROFESSOR GALDE
REASON: CYBER OPERATION PROGRAM
DECYBER ON: OCTOBER 2060

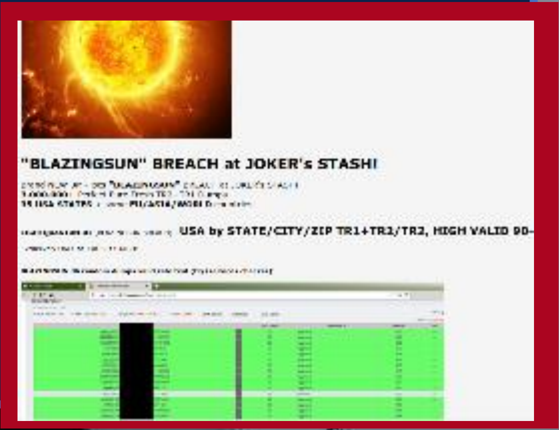
HACKS of THE MONTH

Social Engineering …. Just Works

Multiple cryptocurreny services were hacked by …. Tricking the services webhost. Fraudsters redirected email and web traffic destined for several cryptocurrency trading platforms over two weeks of November. The attacks were facilitated by scams targeting employees at GoDaddy, the world's largest domain name registrar. This latest campaign appears to have begun on or around Nov. 13, with an attack on cryptocurrency trading platform liquid.com.

Hospitals have to worry about a lot and its not all COVID-19, we still have ransomware.

The FBI and the U.S. Department of Homeland Security hastily assembled a conference call with healthcare industry executives warning about an "imminent cybercrime threat to U.S. hospitals and healthcare providers. They warned participants about "credible information of an increased and imminent cybercrime threat to US hospitals and healthcare providers."



"BLAZINGSUN" BREACH at JOKER's STASH!

USA by STATE/CITY/ZIP TR1+TR1/TR2, HIGH VALID 90-

Yummy BBQ and Credit Cards!!

"BlazingSun," a new batch of more than three million stolen card records from the BBQ chain Dickey's which appears to be either unaware of the compromise or has only just begun responding to it. 156 Dickey's locations across 30 states likely had payment systems compromised by card-stealing malware, with the highest exposure in California and Arizona with the exposure window between July 2019 and August 2020.

DEPARTMENT OF DEFENSE

CYBER SCHOLARSHIP

INFORMATIONAL MEETING

VIEW THE INFO MEETING AND LEARN HOW YOU CAN APPLY FOR THE PROGRAM BY VISITING HERE!

- Full cost of tuition and ALL fees provided for 2020-2021 academic year.
- A $25,000 (undergraduate) or $30,000 (graduate) stipend for room and board.
- Covering the cost of all required books (up to $1,250 a year).
- A laptop (up to $1,500).

BASIC REQUIREMENTS

- Minimum cumulative GPA of 3.2 (undergraduate) or 3.5 (graduate).
- Must be entering junior or senior year or a graduate program in Fall 2020.
- Must be a U.S. Citizen.
- Agree to work for the DoD as a civilian for one year for each year of scholarship received.

CYBER NEWS UPDATES

LAWSUITS LIKELY TO CHALLENGE FACEBOOK FOR BUYING RIVALS AND WEAPONIZING DATA

State and federal investigators are preparing to bring antitrust charges against Facebook that will challenge the tech giant's acquisition of two rivals, Instagram and WhatsApp. The charges form a critical part of what could be a wide-ranging legal salvo, according to three people with knowledge of the matter, ultimately threatening to saddle Facebook with its toughest regulatory challenge in its nearly 17-year history.

DISCOVER MORE | CYBV 480 CYBER WARFARE | CYBV 435 Cyber Threat Intelligence | CYBV 385 INTRODUCTION TO CYBER OPERATIONS | CYBV 301 FUNDAMENTALS OF CYBERSECURITY

HACKERS SAID THEY COULD STEAL A TESLA MODEL X IN MINUTES. TESLA PUSHED OUT A FIX.

Belgian researchers found they could hack and steal a Tesla Model X SUV in a matter of minutes through a Bluetooth-connected key fob. They said that forced Tesla to push out a fix. The researchers said they were able to break into the SUV, which starts at $80,000, using a few hundred dollars worth of equipment. The researchers, said Tesla is rolling out an update intended to address the issue. The researchers said that the problem is not necessarily unique to Tesla.

DISCOVER MORE | CYBV 454 MALWARE THREATS & ANALYSIS | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 388 CYBER INVESTIGATIONS AND FORENSICS | CYBV 385 INTRODUCTION TO CYBER OPERATIONS

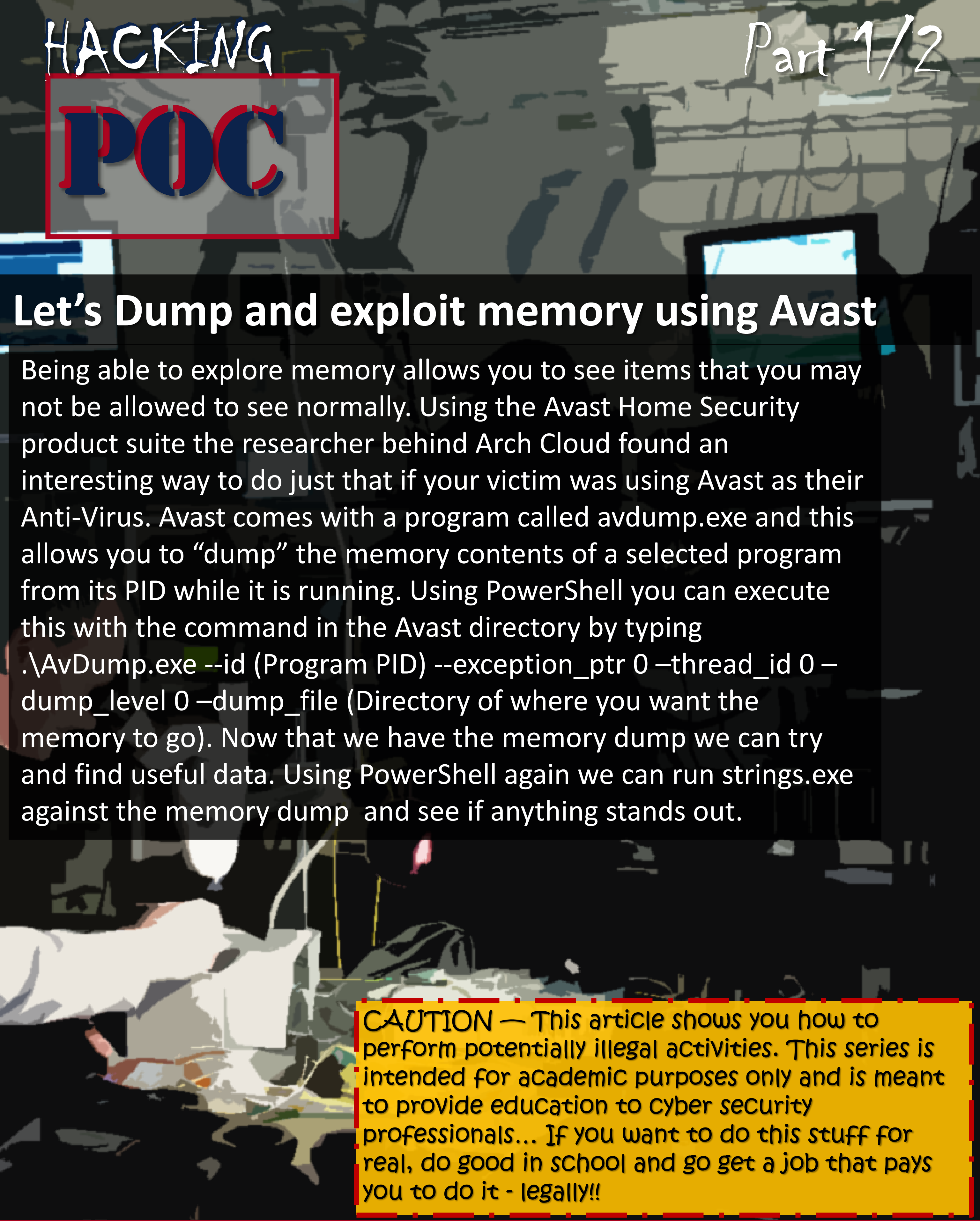
DANISH NEWS AGENCY REJECTS RANSOM DEMAND AFTER HACKER ATTACK

Denmark's biggest news agency will stay offline for at least another day following a hacking attack this week and has rejected a ransom demand by hackers to release locked data. Ritzau CEO Lars Vesterloekke couldn't say how big the ransom demand was because those behind the "professional attack" had left "a file with a message" that the agency didn't open following instructions from its advisers.

DISCOVER MORE | CYBV 436 COUNTER CYBER THREAT INTELLIGENCE | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 329 CYBER ETHICS | CYBV 385 INTRODUCTION TO CYBER OPERATIONS

CYBER OPERATIONS SPRING 2021

CAT #	COURSE	Books
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	Book
CYBV 310	INTRO SECURITY PROGRAMMING I	Book
CYBV 311	INTRO SECURITY PROGRAMMING II	Book
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	Book
CYBV 326	INTRO METHODS OF NETWORKING ANALYSIS	Book
CYBV 329	CYBER ETHICS	Book
CYBV 354	PRINCIPLES OPEN-SOURCE INTEL	Book
CYBV 385	INTRO TO CYBER OPERATIONS	Book
CYBV 381	INCIDENT RESPONSE TO DIGITAL FORENSICS	Book
CYBV 382	NETWORK FORENSICS	Book
CYBV 388	CYBER INSTIGATIONS AND FORENSICS	Book 1, Book 2
CYBV 400	ACTIVE CYBER DEFENSE	Book 1, Book 2
CYBV 435	CYBER THREAT INTELLIGENCE	Book 1, Book 2, Book 3
CYBV 436	COUNTER CYBER THREAT INTEL	Book
CYBV 437	DECEPTION & COUNTER-DECEPTION	Book
CYBV 440	DIGITAL ESPIONAGE	Book 1, Book 2
CYBV 441	CYBER WAR, TERROR AND CRIME	Book 1, Book 2
CYBV 450	INFORMATION WARFARE	Book 1
CYBV 454	MALWARE THREATS & ANALYSIS	Book
CYBV 471	ASSEMBLY LANG PROG FOR SEC PROF	Book
CYBV 473	VIOLENT PYTHON	Book 1, Book 2
CYBV 474	ADVANCED ANALYTICS FOR SEC OPS	Book 1, Book 2
CYBV 480	CYBER WARFARE	Book 1, Book 2
CYBV 481	SOC ENG ATTACK & DEFENSE	Book 1, Book 2
CYBV 496	SPCL TOPICS IN CYBER SECURITY	Book



HACKING

POC

Part 1/2

Let’s Dump and exploit memory using Avast

Being able to explore memory allows you to see items that you may not be allowed to see normally. Using the Avast Home Security product suite the researcher behind Arch Cloud found an interesting way to do just that if your victim was using Avast as their Anti-Virus. Avast comes with a program called avdump.exe and this allows you to “dump” the memory contents of a selected program from its PID while it is running. Using PowerShell you can execute this with the command in the Avast directory by typing .\AvDump.exe --id (Program PID) --exception_ptr 0 –thread_id 0 – dump_level 0 –dump_file (Directory of where you want the memory to go). Now that we have the memory dump we can try and find useful data. Using PowerShell again we can run strings.exe against the memory dump and see if anything stands out.

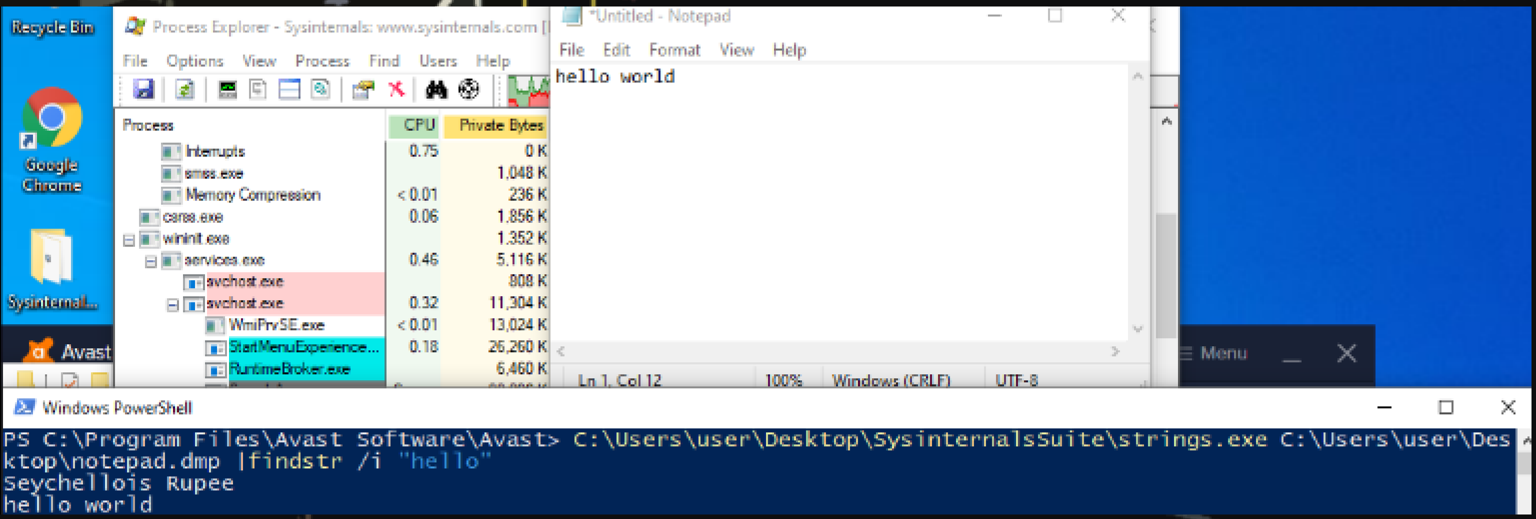
CAUTION — This article shows you how to perform potentially illegal activities. This series is intended for academic purposes only and is meant to provide education to cyber security professionals... If you want to do this stuff for real, do good in school and go get a job that pays you to do it - legally!!

HACKING POC

Part 1/2

Let’s Dump and exploit memory using Avast

The researcher used notepad as an example and wrote the message “Hello World” inside of it. Now this is a document that is not saved but is running in system memory. So by running AvDump.exe against the PID of notepad.exe we were able to capture what was being held in memory. By running strings.exe against this memory capture we can extract data allowing us to see what was inside. Now this can be applied to different programs that is running and if a “victim” is running this software you would have a technique available to you which allows you to see what system memory is holding, this could be anything from system credentials depending how they are stored and processed, or messages not intended for saving on the local machine. Either way dumping memory allows you to bypass many mitigations if you have this level of access to a machine you would not normally have access to.


Recycle Bin
Google Chrome
Sysinternal...
Avast
Process Explorer - Sysinternals: www.sysinternals.com
File Options View Process Find Users Help
*Untitled - Notepad
File Edit Format View Help
Menu
Windows PowerShell

Process	CPU	Private Bytes
Interrupts	0.75	0 K
smss.exe		1,048 K
Memory Compression	< 0.01	236 K
csrss.exe	0.06	1,856 K
wininit.exe		1,352 K
services.exe	0.46	5,116 K
svchost.exe		808 K
svchost.exe	0.32	11,304 K
WmiPrvSE.exe	< 0.01	13,024 K
StartMenuExperience...	0.18	26,260 K
RuntimeBroker.exe		6,460 K

```
hello world
```

Ln 1, Col 12 100% Windows (CRLF) UTF-8

```
PS C:\Program Files\Avast Software\Avast> C:\Users\user\Desktop\SysinternalsSuite\strings.exe C:\Users\user\Des
ktop\notepad.dmp |findstr /i "hello"
Seychellois Rupee
hello world
```

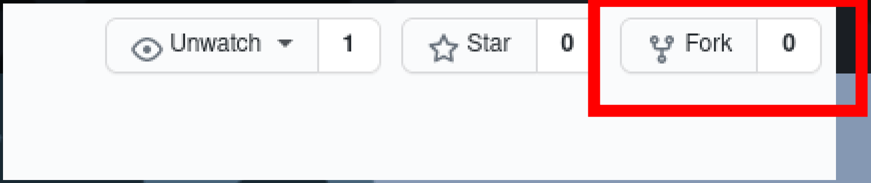
QUICK PROJECT

Custom Start Page

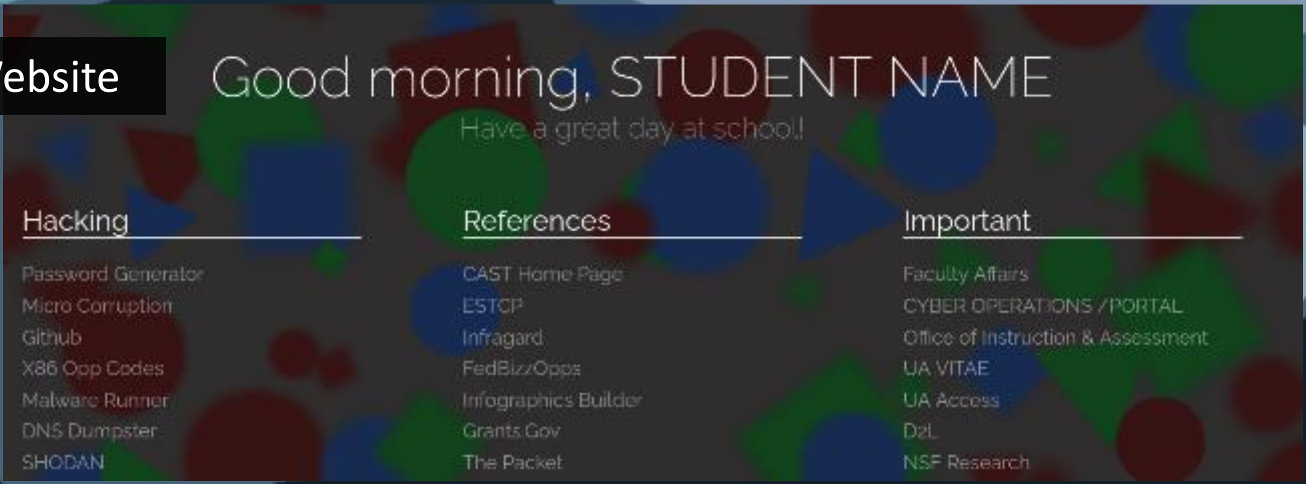
Part 1/6

LET'S MAKE A SIMPLE STARTPAGE

So every day I start my computer and begin my day and log into my various services to start my day. Its almost as constant as my morning coffee. I also hate bookmarks; I have nothing against them I just do not like the way they look. In my many travels through the world wide web I came across a Reddit group called /r/startpages. It was from here that the solution for me was so simple. I should create a website that did nothing but hold the links that I cared about. Well today I will show you how to create your very own and set it up as your websites home page. So now when you start your computer and start to log into your various services you have a one stop shop to start from. The first thing you will need is to establish a Github account and fork my example by clicking my example here.



Demo Website



Good morning, STUDENT NAME

Have a great day at school!

Hacking
- Password Generator
- Micro Corruption
- Github
- X86 Opp Codes
- Malware Runner
- DNS Dumpster
- SHODAN

References
- CAST Home Page
- ESTCP
- Infragard
- FedBizzOpps
- Infographics Builder
- Grants.Gov
- The Packet

Important
- Faculty Affairs
- CYBER OPERATIONS / PORTAL
- Office of Instruction & Assessment
- UA VITAE
- UA Access
- D2L
- NSF Research

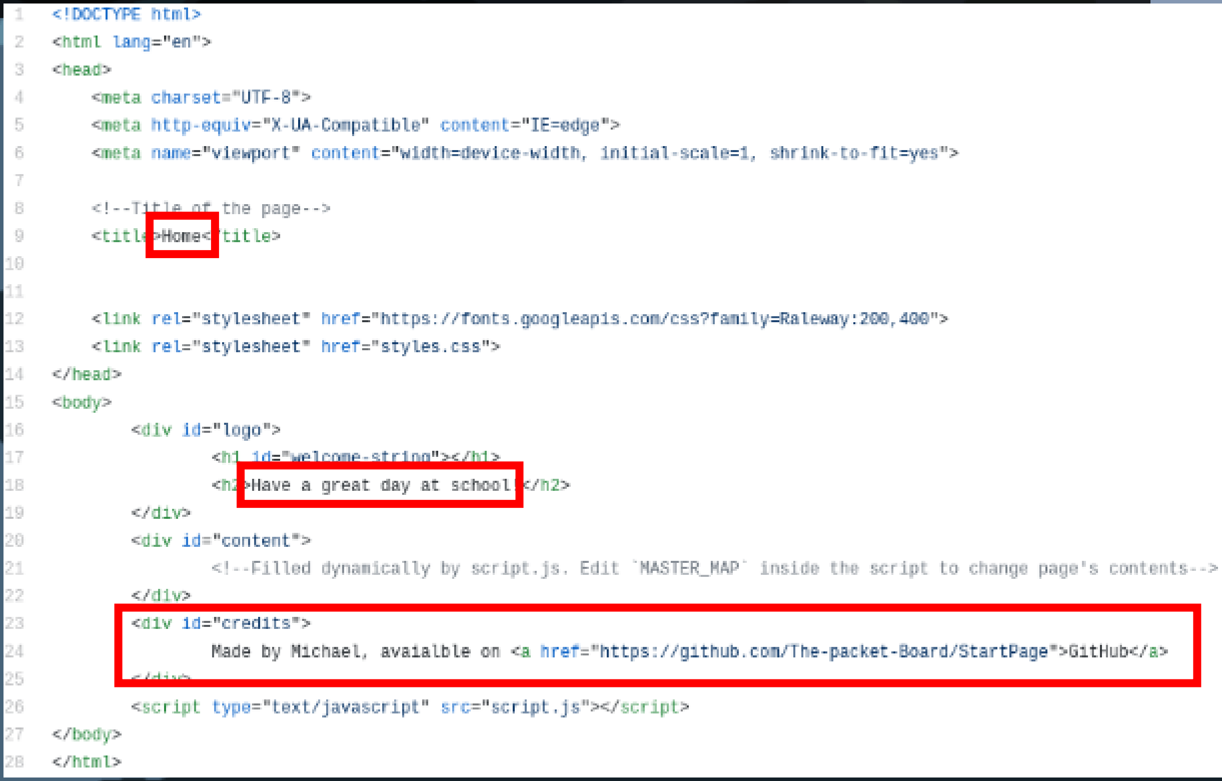
QUICK PROJECT

Custom Start Page

Part 2/6

EDIT INDEX.HTML

Index.html is what your web browser requests when it goes to your link, for our cases you only need to edit a few lines to fit your preference. On line 9 you can change Home to what ever you would like your webpage to be called. This is a preference to you, and you can easily leave it alone. Next on line 18 is the welcome message, you can again change this to something better suited to you. Finally, on line 23 to 24 you can add your details so anyone that comes across your page knows who made it. Again, this is a preference. The Index.html page then makes a call to script.js and this is where most of the magic happens, that is what we will edit next on the next page.



```
1  <!DOCTYPE html>
2  <html lang="en">
3  <head>
4      <meta charset="UTF-8">
5      <meta http-equiv="X-UA-Compatible" content="IE=edge">
6      <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=yes">
7
8      <!--Title of the page-->
9      <title>Home</title>
10
11
12     <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Raleway:200,400">
13     <link rel="stylesheet" href="styles.css">
14 </head>
15 <body>
16         <div id="logo">
17                 <h1 id="welcome-string"></h1>
18                 <h2>Have a great day at school!</h2>
19         </div>
20         <div id="content">
21                 <!--Filled dynamically by script.js. Edit `MASTER_MAP` inside the script to change page's contents-->
22         </div>
23         <div id="credits">
24                 Made by Michael, avaialble on <a href="https://github.com/The-packet-Board/StartPage">GitHub</a>
25         </div>
26         <script type="text/javascript" src="script.js"></script>
27 </body>
28 </html>
```

QUICK PROJECT

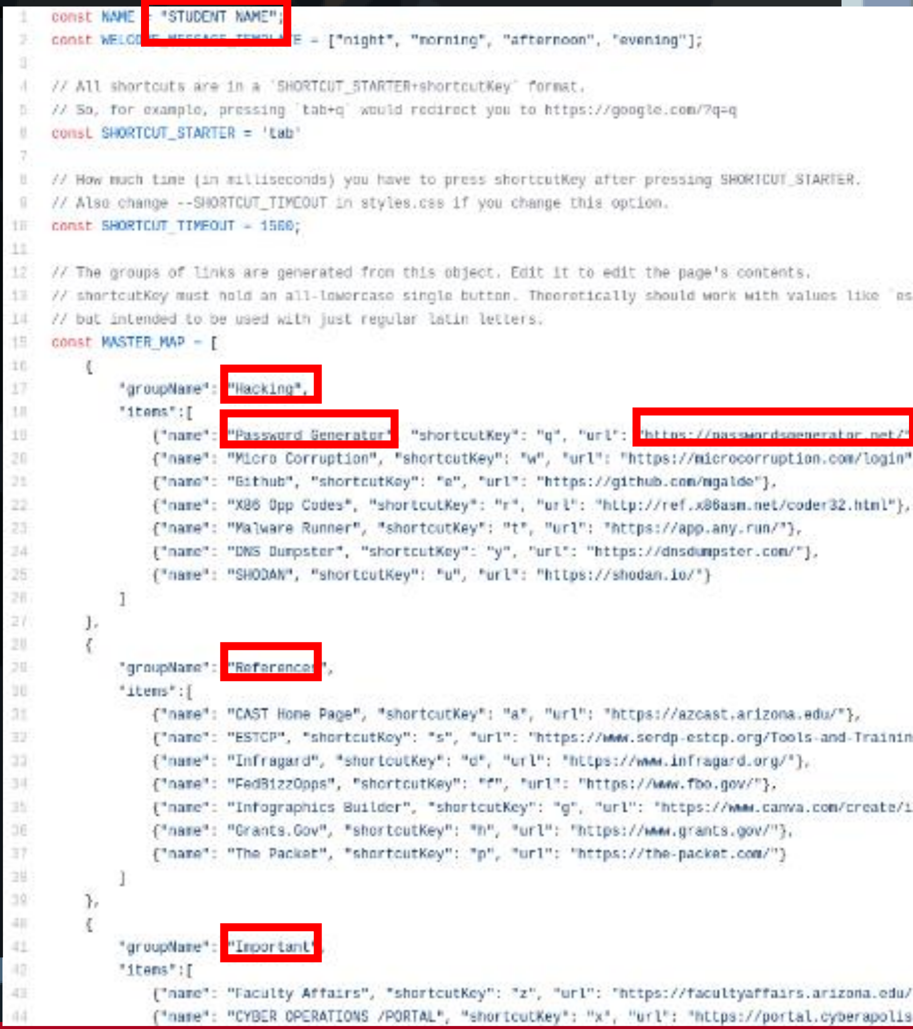
Custom Start Page

Part 3/6

EDIT SCRIPT.JS

Think of script.js as the logic that the website displays, it may look intimidating, but I hope to explain what to change to where anyone would be able to have their own page custom to you. So first, on line 1 change the STUDENT NAME to what you would like to be called. I have my links separated into 3 fields; Hacking, References and Important. You can rename these fields to whatever you wish.

Discover the links you want to add and then change them in the name field and then the URL. I also include keyboard shortcuts and feel free to change these as you see fit. The rest of the logic does not need to be customized or edited but if you are feeling daring you could adjust other details in this page, though for this quick example we will not break that down. Next, we will adjust the background in styles.css.



```
1   const NAME = "STUDENT NAME";
2   const WELCOME_MESSAGE_TEMPLATE = ["night", "morning", "afternoon", "evening"];
3
4   // All shortcuts are in a `SHORTCUT_STARTER+shortcutKey` format.
5   // So, for example, pressing `tab+q` would redirect you to https://google.com/?q=q
6   const SHORTCUT_STARTER = 'tab'
7
8   // How much time (in milliseconds) you have to press shortcutKey after pressing SHORTCUT_STARTER.
9   // Also change --SHORTCUT_TIMEOUT in styles.css if you change this option.
10  const SHORTCUT_TIMEOUT = 1500;
11
12  // The groups of links are generated from this object. Edit it to edit the page's contents.
13  // shortcutKey must hold an all-lowercase single button. Theoretically should work with values like `es
14  // but intended to be used with just regular latin letters.
15  const MASTER_MAP = [
16      {
17          "groupName": "Hacking",
18          "items":[
19              {"name": "Password Generator", "shortcutKey": "q", "url": "https://passwordsgenerator.net/"
20              {"name": "Micro Corruption", "shortcutKey": "w", "url": "https://microcorruption.com/login"
21              {"name": "Github", "shortcutKey": "e", "url": "https://github.com/mgalde"},
22              {"name": "X86 Opp Codes", "shortcutKey": "r", "url": "http://ref.x86asm.net/coder32.html"},
23              {"name": "Malware Runner", "shortcutKey": "t", "url": "https://app.any.run/"},
24              {"name": "DNS Dumpster", "shortcutKey": "y", "url": "https://dnsdumpster.com/"},
25              {"name": "SHODAN", "shortcutKey": "u", "url": "https://shodan.io/"}
26          ]
27      },
28      {
29          "groupName": "References",
30          "items":[
31              {"name": "CAST Home Page", "shortcutKey": "a", "url": "https://azcast.arizona.edu/"},
32              {"name": "ESTCP", "shortcutKey": "s", "url": "https://www.serdp-estcp.org/Tools-and-Trainin
33              {"name": "Infragard", "shortcutKey": "d", "url": "https://www.infragard.org/"},
34              {"name": "FedBizzOpps", "shortcutKey": "f", "url": "https://www.fbo.gov/"},
35              {"name": "Infographics Builder", "shortcutKey": "g", "url": "https://www.canva.com/create/i
36              {"name": "Grants.Gov", "shortcutKey": "h", "url": "https://www.grants.gov/"},
37              {"name": "The Packet", "shortcutKey": "p", "url": "https://the-packet.com/"}
38          ]
39      },
40      {
41          "groupName": "Important",
42          "items":[
43              {"name": "Faculty Affairs", "shortcutKey": "z", "url": "https://facultyaffairs.arizona.edu/
44              {"name": "CYBER OPERATIONS /PORTAL", "shortcutKey": "x", "url": "https://portal.cyberapolis
```

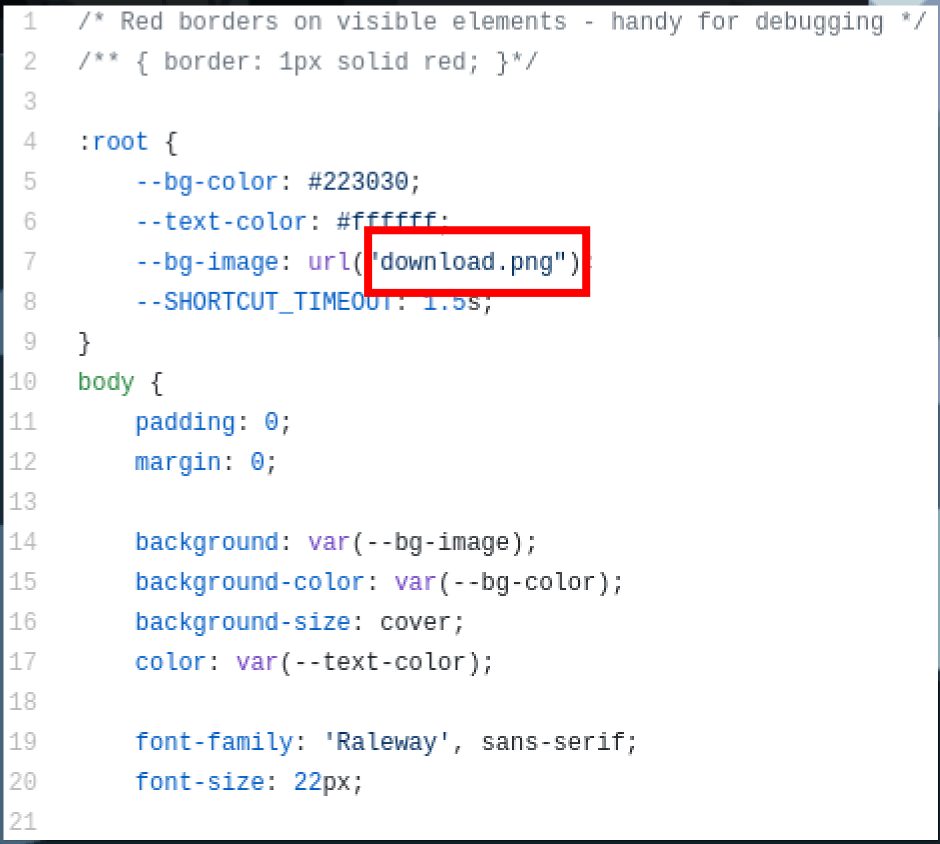
QUICK PROJECT

Custom Start Page

Part 4/6

EDIT STYLES.CSS

Styles.css tells the web browser how to present your page. For our example we are going to change the background image. This is under line 7 and the image is labeled download.png. You can keep this as you wish, or you can download your own image and make sure it is referenced in this area. Now when your page loads, the background will be loaded from these calls. You should self host your own images by uploading them to your repository so that you are not linking to websites you do not control. Next, we will set up GitHub to host your amazing website.



```
1   /* Red borders on visible elements - handy for debugging */
2   /** { border: 1px solid red; }*/
3
4   :root {
5       --bg-color: #223030;
6       --text-color: #ffffff;
7       --bg-image: url("download.png");
8       --SHORTCUT_TIMEOUT: 1.5s;
9   }
10  body {
11      padding: 0;
12      margin: 0;
13
14      background: var(--bg-image);
15      background-color: var(--bg-color);
16      background-size: cover;
17      color: var(--text-color);
18
19      font-family: 'Raleway', sans-serif;
20      font-size: 22px;
21
```

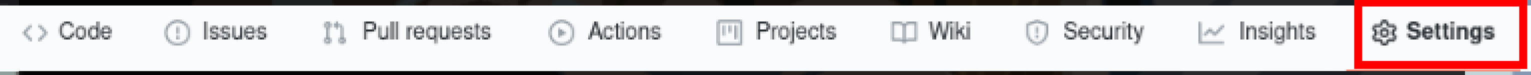
QUICK PROJECT

Custom Start Page

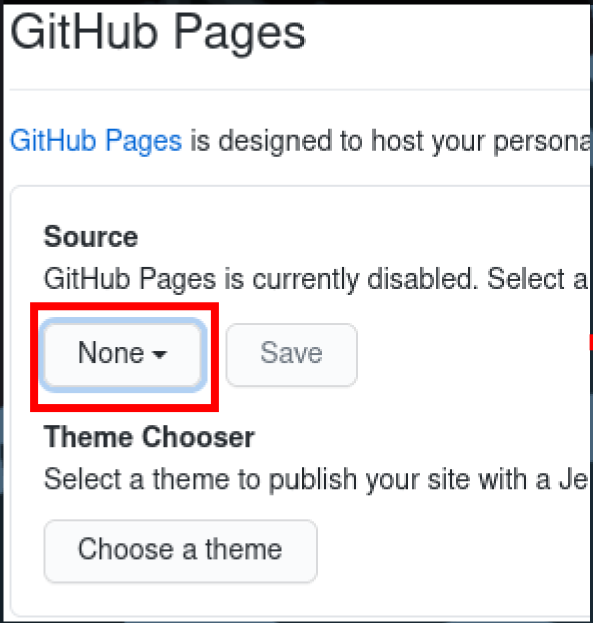
Part 5/6

HOST YOUR WEBSITE ON GITHUB

Now that we have all the code you want modified; we want GitHub to host our website. There is a series of links and you want to click on the settings tab.



Now we scroll down to find the GitHub Pages settings and we will click where it says "None" and select "Main"


GitHub Pages

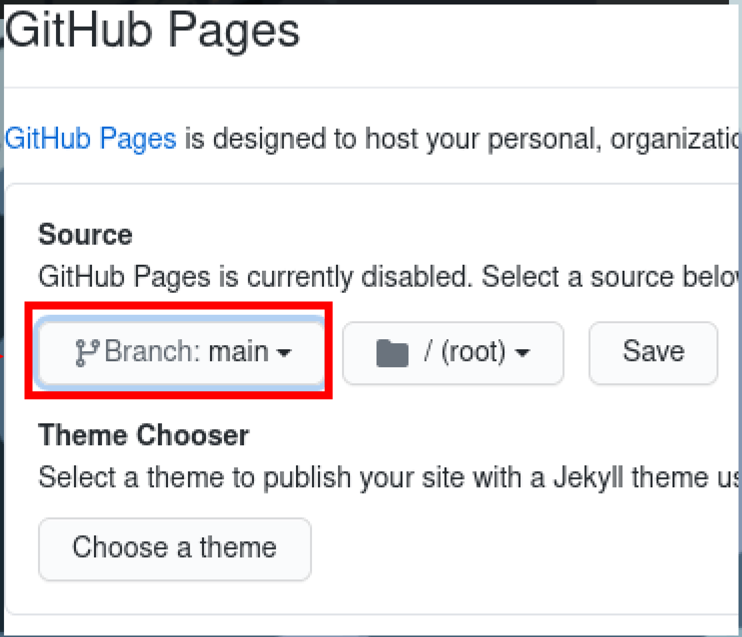
GitHub Pages is designed to host your persona

Source

GitHub Pages is currently disabled. Select a

Theme Chooser

Select a theme to publish your site with a Je


GitHub Pages

GitHub Pages is designed to host your personal, organizatio

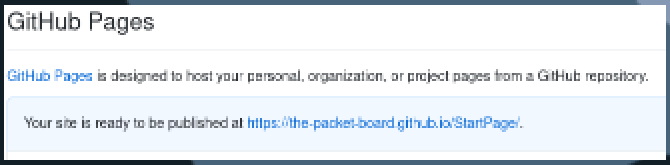
Source

GitHub Pages is currently disabled. Select a source belo

Theme Chooser

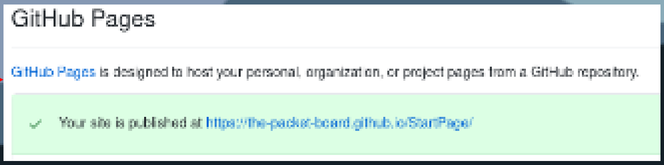
Select a theme to publish your site with a Jekyll theme us

Finally we will click save and make note of the web address that GitHub gives us. Refresh the page a few times tell this background turns green.


GitHub Pages

GitHub Pages is designed to host your personal, organization, or project pages from a GitHub repository.

Your site is ready to be published at https://the-packet-board.github.io/StartPage/.


GitHub Pages

GitHub Pages is designed to host your personal, organization, or project pages from a GitHub repository.

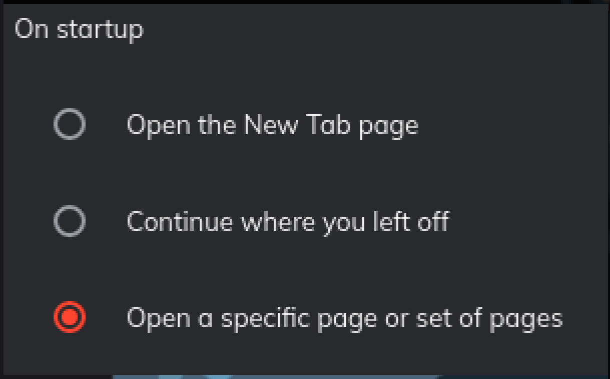
✓ Your site is published at https://the-packet-board.github.io/StartPage/

QUICK PROJECT

Custom Start Page
Part 6/6

MAKE YOUR WEBPAGE YOUR HOMEPAGE

Now that GitHub is hosting our page, we need to add this as our home page. Every web browser is different, but they usually follow the same path. Under your browser settings you want to select a custom URL home page. Under Chrome or Brave you will see this under settings when you first open up the menu labeled “On Startup”.

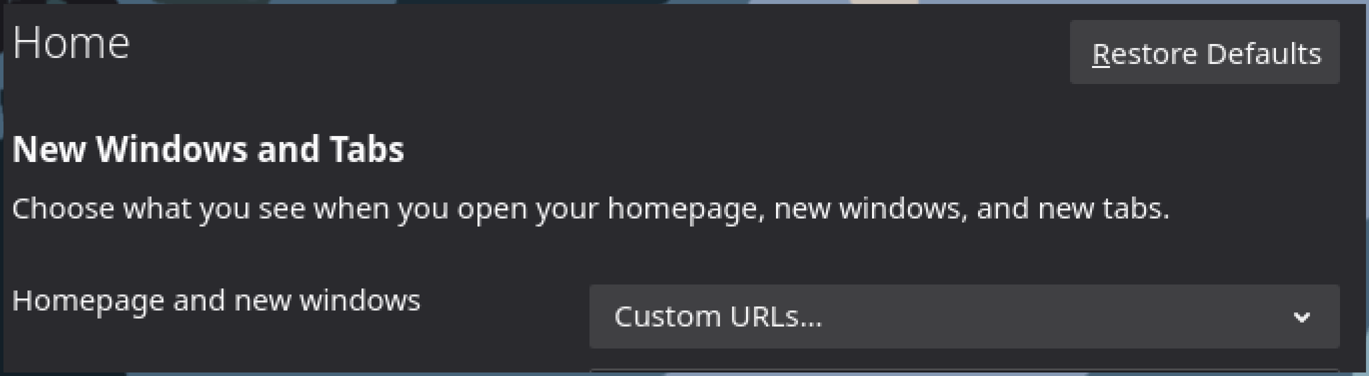

On startup

○ Open the New Tab page

○ Continue where you left off

● Open a specific page or set of pages

Under Firefox you would navigate to preferences and then the Home Tab and edit the Home setting with a Custom URL. Now enter your GitHub URL and you are greeted with your own custom “Bookmark” page that will be made for you.


Home

New Windows and Tabs

Choose what you see when you open your homepage, new windows, and new tabs.

Homepage and new windows: Custom URLs...

Play and make your own examples, and then submit to me your creations. I may end up doing a collection of what everyone has made in a future edition of The Packet.

CYBER SECURITY HISTORY

LAROUX, THE FIRST EXCEL MACRO VIRUS DECEMBER 1, 1996

Laroux was a simple virus, living in Microsoft Excel it would look for files labeled PERSONAL.XLS and if it found it add itself as a macro. Laroux would than infect any Excel document that the victim saved or accessed. PERSONAL.XLS is a record of all macros available to all Microsoft Excel documents as a convenience feature. This however is how this virus would spread. This was more of a concept then a malicious attack and was only observed in Alaska and South Africa. No indication is given as to whether the virus originated from one of these locations and these locations were offices of oil companies. The companies were reportedly paralyzed.

AIDS TROJAN – FIRST RANSOMWARE DECEMBER 19, 1989

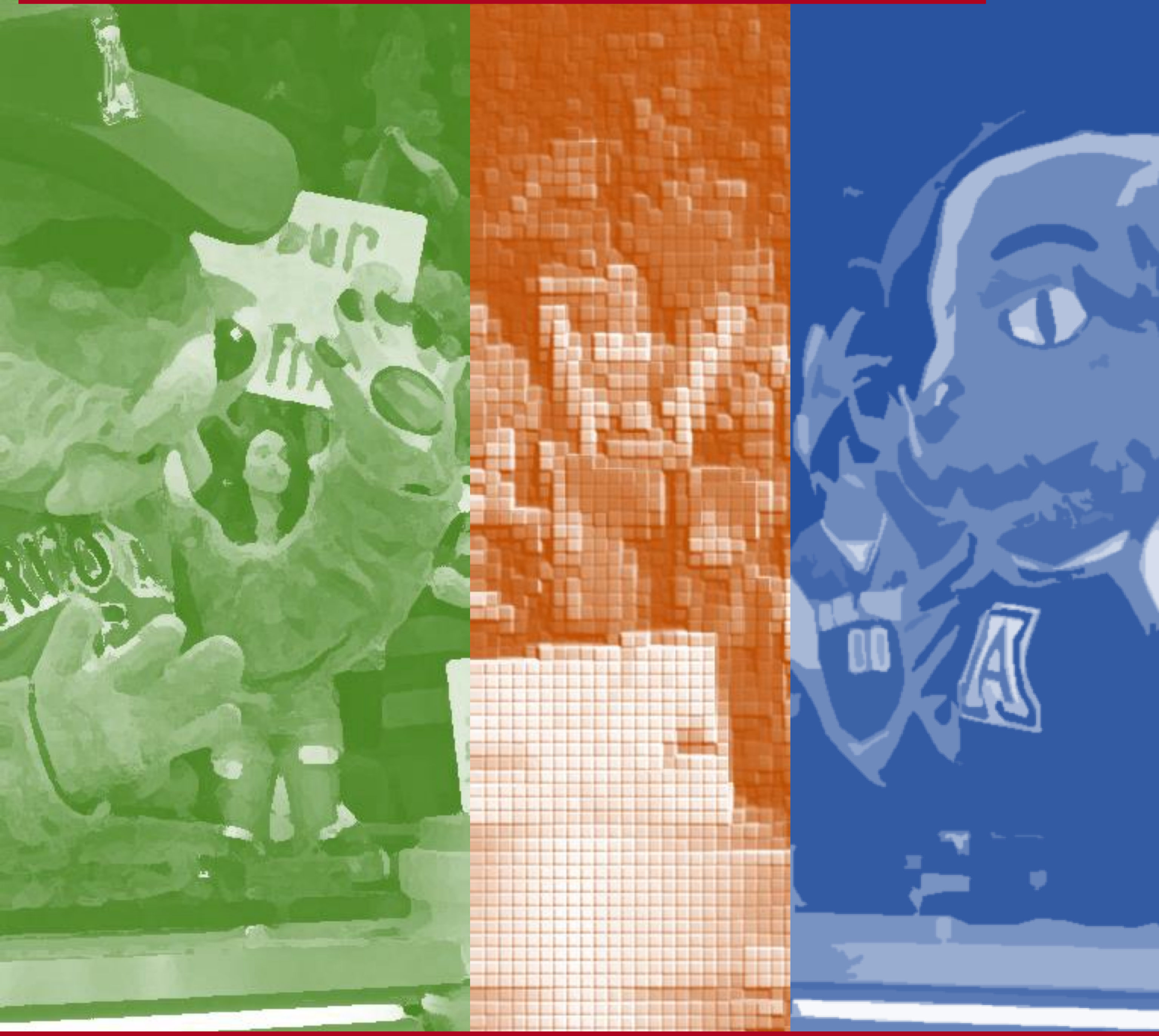
AIDS or also known as the PC Cyborg Trojan compromises the autoexec.bat file and counts how many times a DOS machine boots up. When 90 boots have been recorded AIDS then encrypts files on the C Drive and hides directories. It then asks for $189 US to be sent to a Panama address. This was created by Evolutionary biologist Dr. Joseph Popp who claims that all payments would go to AIDS research. Dr. Popp was charged with eleven counts of blackmail by British authorities but was declared mentally unfit to stand trial and was returned to the United States.

PCI DSS 1.0 LAUNCHED DECEMBER 15, 2004

PCI DSS or Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. If you were an organization that wanted to take in credit card transactions, you must be PCI DSS compliant. MasterCard, American Express, Visa, JCB International and Discover Financial Services established the PCI SSC (Security Standards Council) in September 2006 as an administration/governing entity which mandates the evolution and development of PCI DSS. This security standard is now in version 3.2.1 and was created to increase controls around cardholder data to reduce credit card fraud.

THE PACKET

THE UNIVERSITY OF ARIZONA



CONTACT US

CIIO@EMAIL.ARIZONA.EDU

1140 N. Colombo Ave. | Sierra Vista, AZ 85635

Phone: 520-458-8278 ext 2155

http://cyber-operations.azcast.arizona.edu/

THE UNIVERSITY OF ARIZONA