

Emerging Cyber Threats & Attacks

Hari Haran, NIC-CERT



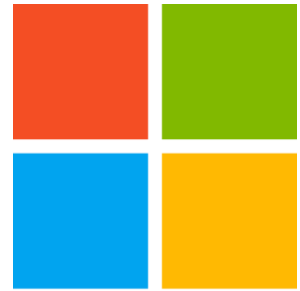
Agenda



- 1 Recent Security Incidents
- 2 Emerging Security Threats
- 3 Case Studies
- 4 Homograph & Cryptojacking

Recent Security Incidents

Major Cyber Incidents in 2021



Microsoft

acer



Colonial Pipeline Company

Domino's Data Breach

5

Domino's Data Breach

Search your phone number or mailid.

180M rows searchable. Payment details and employee files will be made public soon...

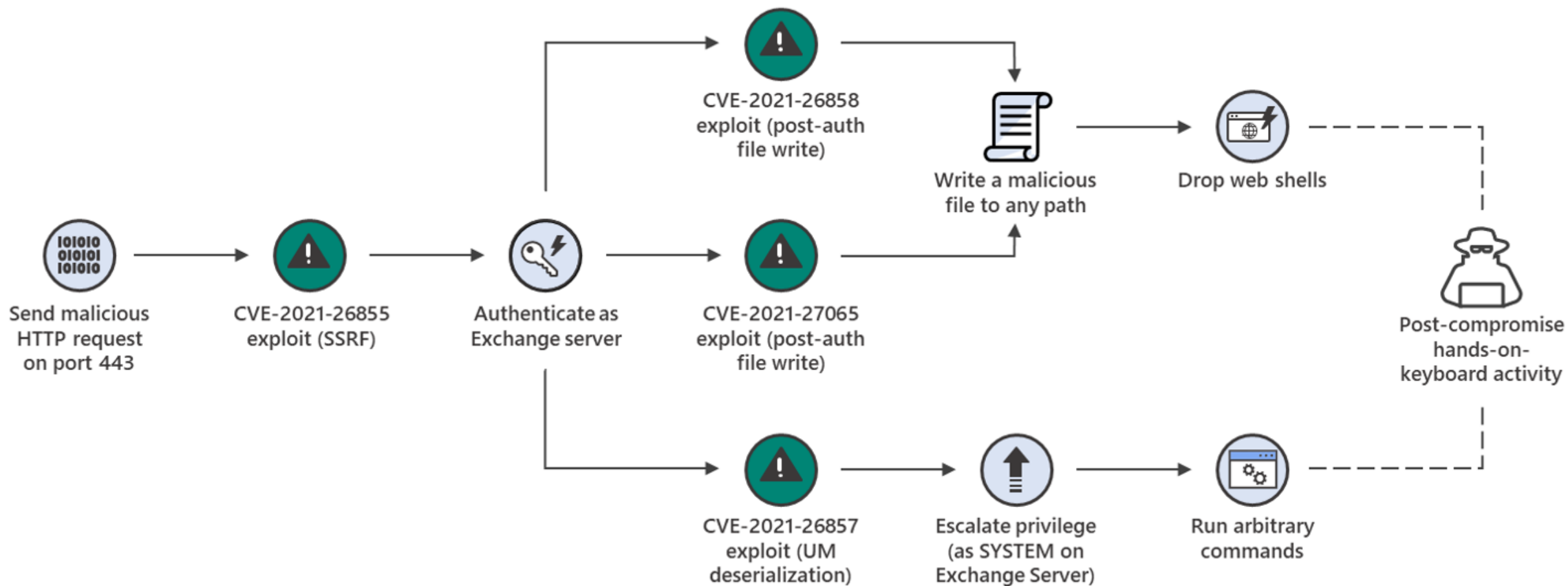
Sample search terms: "9876501234" or "+91 98765 01234" or "john@gmail.com"

Search



Domino's®

Microsoft Exchange Massive Exploitation



Acer Ransomware Attack

7

Happy Blog

Auction (new)

Blog search

Search

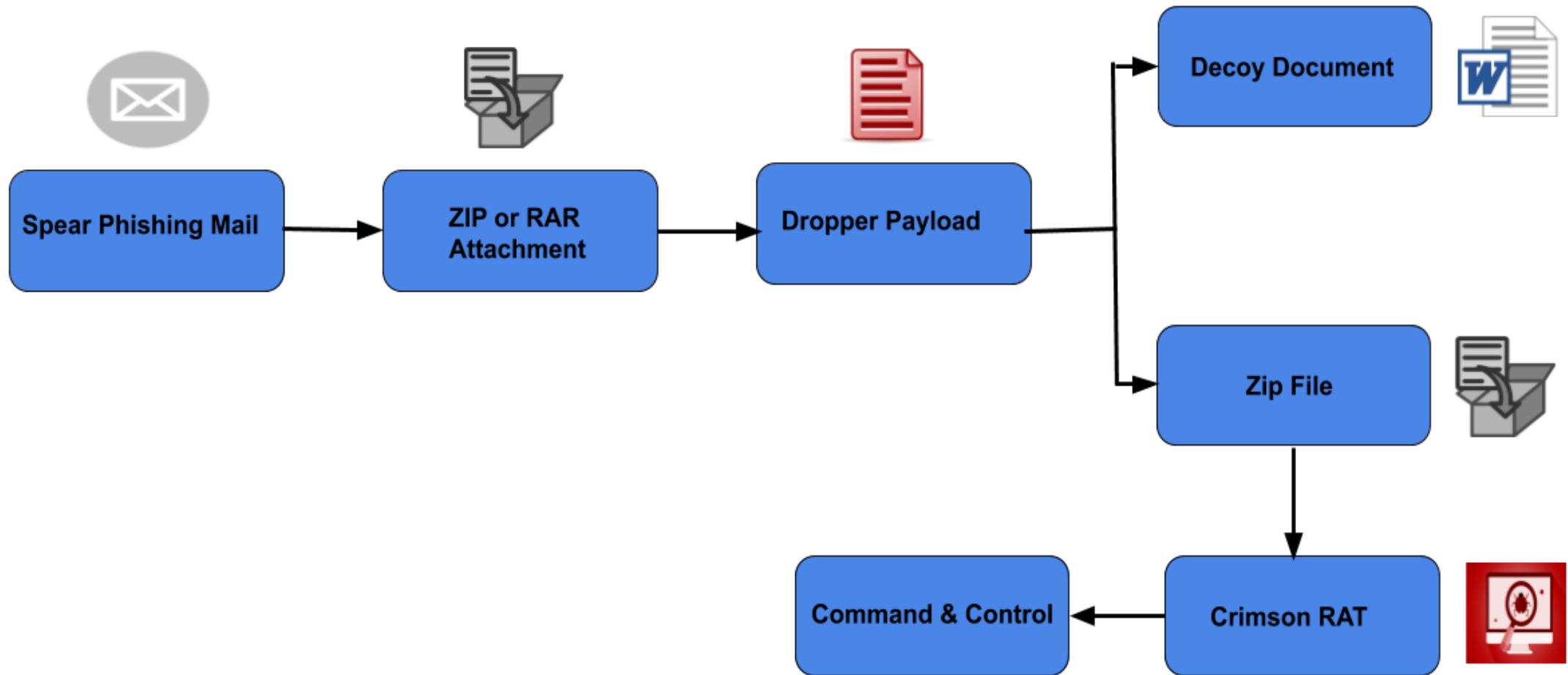
Acer Inc.



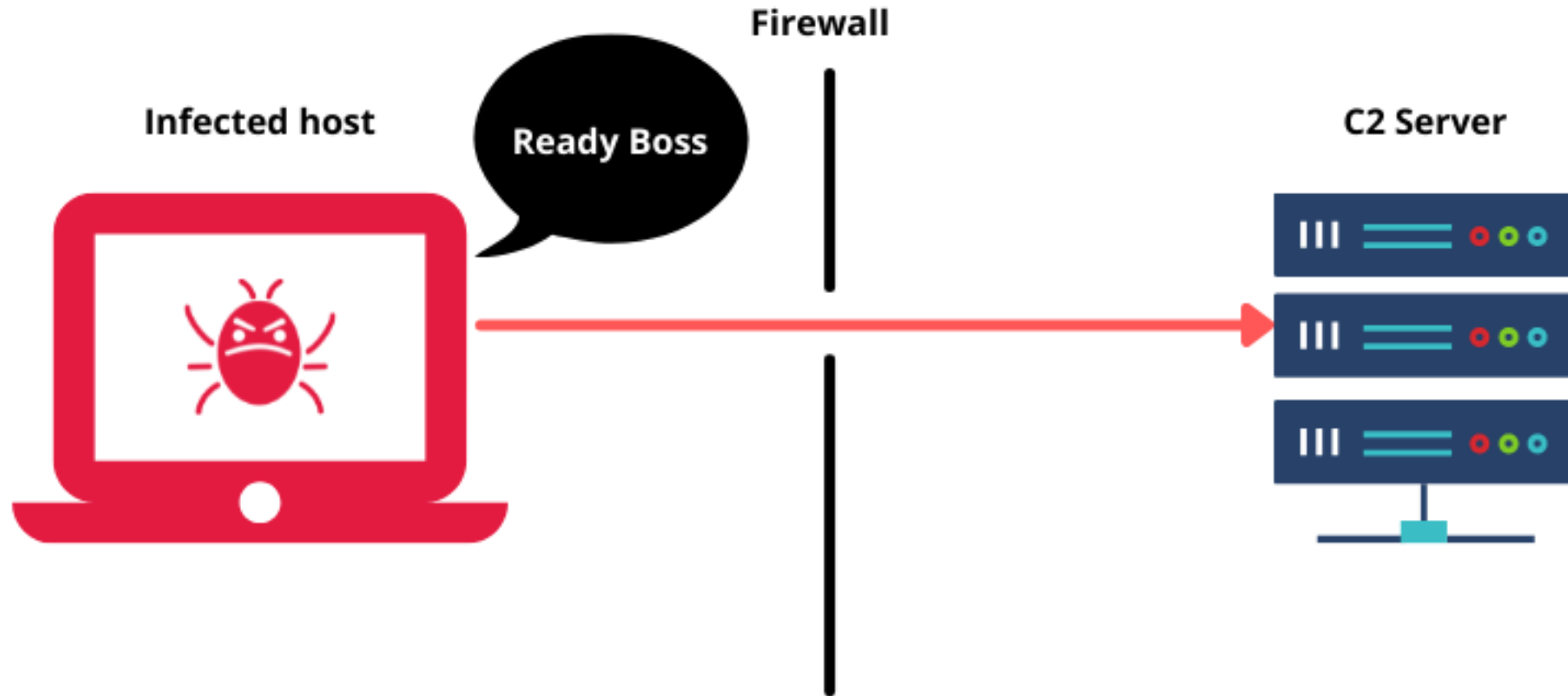
Acer.com - is a Taiwanese multinational hardware and electronics corporation specializing in advanced electronics technology, headquartered in Xizhi, New Taipei City. Its products include desktop PCs, laptop PCs tablets, servers, storage devices, virtual reality devices, displays, smartphones and peripherals, as well as gaming PCs and accessories under its Predator brand. Acer is the world's 6th-largest PC vendor by unit sales as of January 2021

CUSTOMER_CODE		One Customer with multiple Location (Y/N)		Credit Currency	Site Credit Limit	CUSTOMER_NAME	CUSTOMER_LOCAL_NAME
10000011	8 digital Account	N	USD	-	-	Acer Inc.	Acer Inc.
10000017	10000017	N	USD	-	-	Acer Inc.	Acer Inc.
10000022	10000022	N	JPY	-	-	Acer Inc.	Acer Inc.
10000030	10000030	N	USD	-	-	Acer Inc.	Acer Inc.
10000037	10000037	N	JPY	-	-	Acer Inc.	Acer Inc.
10000042	10000042	N	USD	-	-	Acer Inc.	Acer Inc.
10000051	10000051	N	USD	-	-	Acer Inc.	Acer Inc.
10000056	10000056	N	USD	-	-	Acer Inc.	Acer Inc.
10000057	10000057	N	USD	-	-	Acer Inc.	Acer Inc.
10000059	10000059	N	USD	-	-	Acer Inc.	Acer Inc.
10000069	10000069	N	USD	-	-	Acer Inc.	Acer Inc.
10000097	10000097	N	USD	-	-	Acer Inc.	Acer Inc.
10000120	10000120	N	USD	-	-	Acer Inc.	Acer Inc.
10000182	10000182	N	USD	-	-	Acer Inc.	Acer Inc.
10000189	10000189	N	USD	-	-	Acer Inc.	Acer Inc.
10000192	10000192	N	USD	-	-	Acer Inc.	Acer Inc.
10000293	10000293	N	USD	-	-	Acer Inc.	Acer Inc.
10000336	10000336	N	USD	-	-	Acer Inc.	Acer Inc.
10032452	10032452	N	JPY	-	-	Acer Inc.	Acer Inc.
10032453	10032453	Y	JPY	-	-	Acer Inc.	Acer Inc.
10032486	10032486	N	JPY	-	-	Acer Inc.	Acer Inc.
10032544	10032544	N	JPY	-	-	Acer Inc.	Acer Inc.
10032545	10032545	N	JPY	-	-	Acer Inc.	Acer Inc.
10032546	10032546	Y	JPY	-	-	Acer Inc.	Acer Inc.
10032546	10032546	Y	USD	-	-	Acer Inc.	Acer Inc.

Malware Infection – Modus Operandi

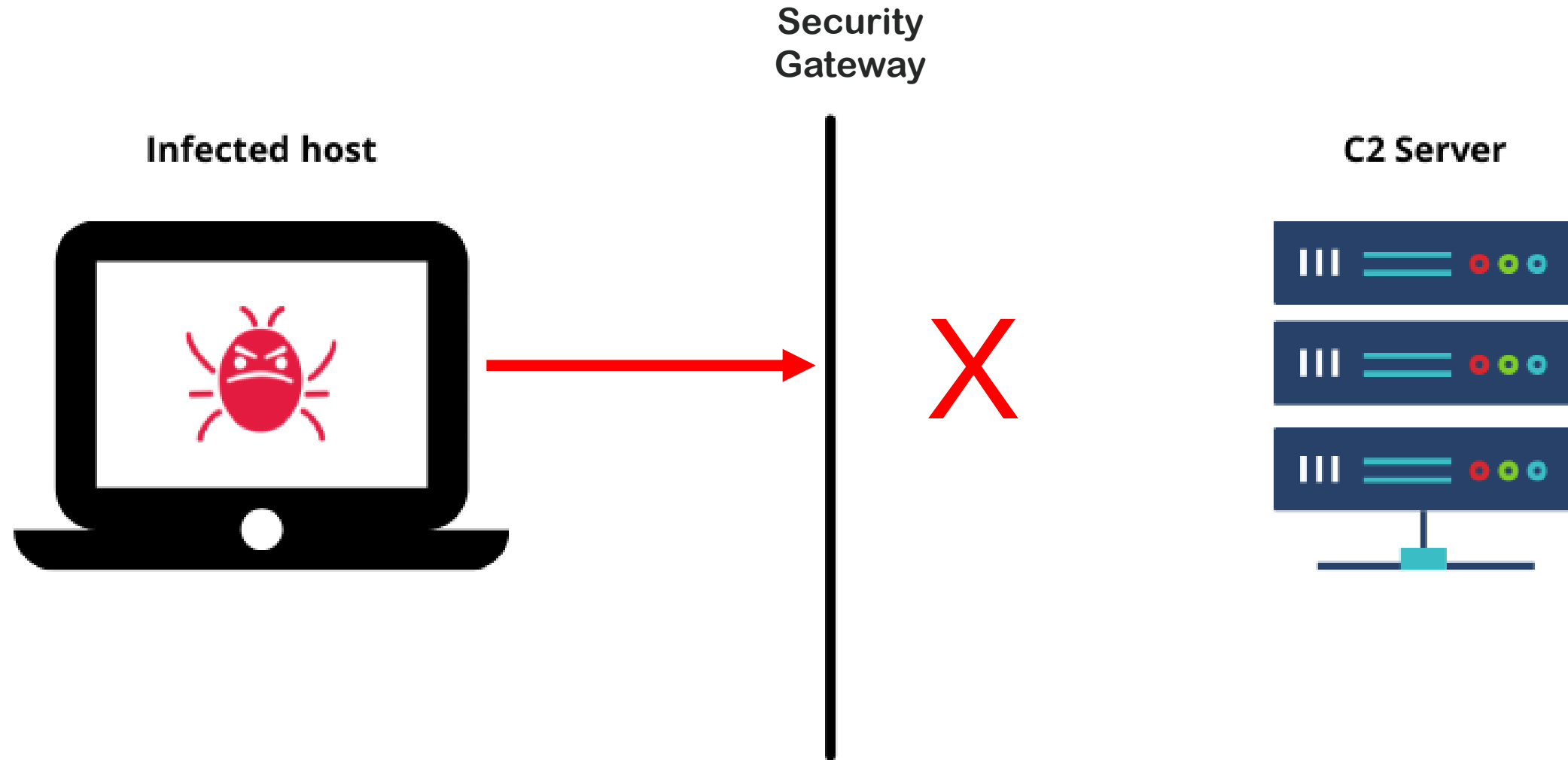


Command & Control - C2 Communication



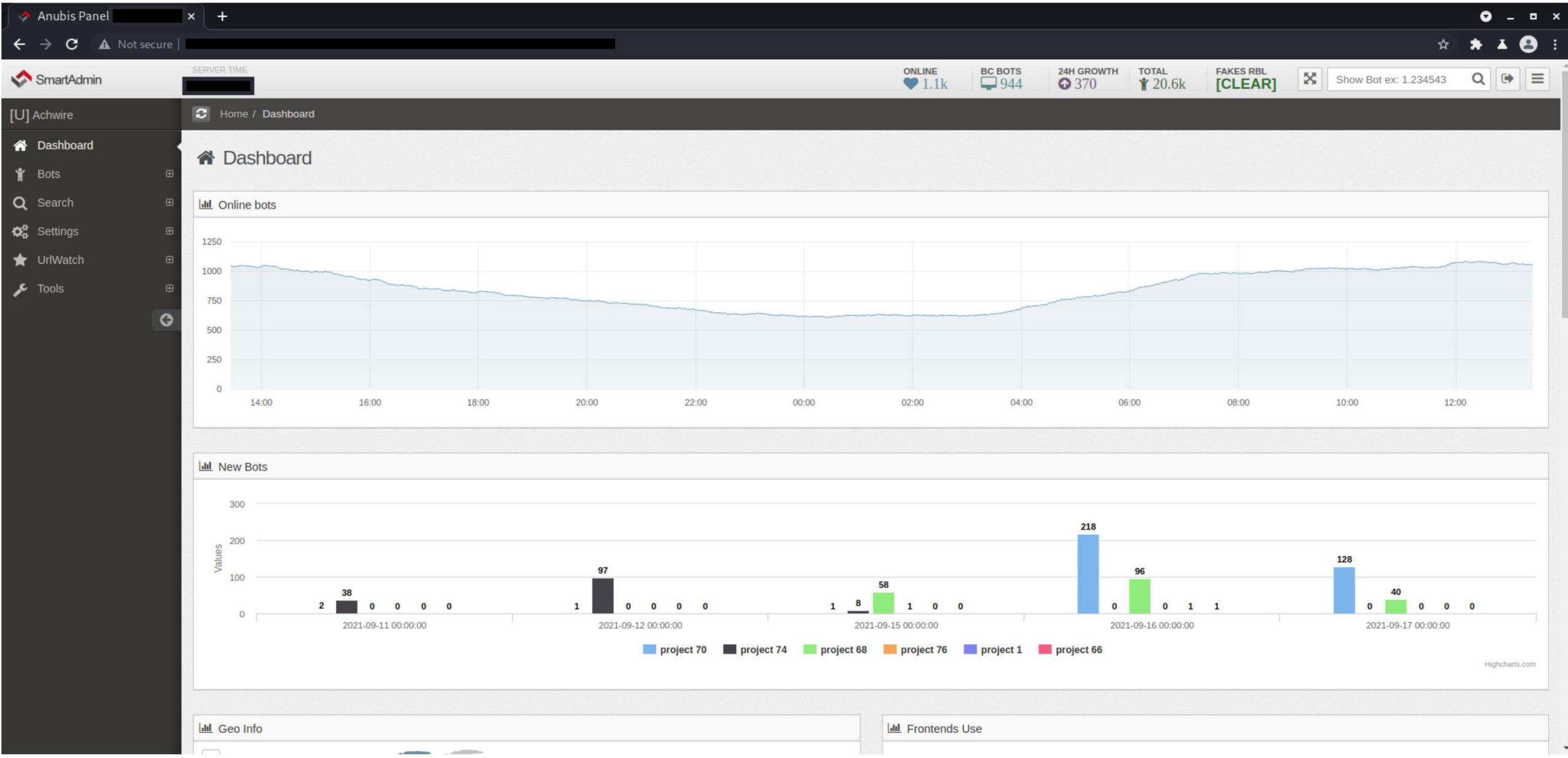
Command & Control - C2 Communication

10



C2 Admin Panel

11



C2 Admin Panel

12

Anubis Panel

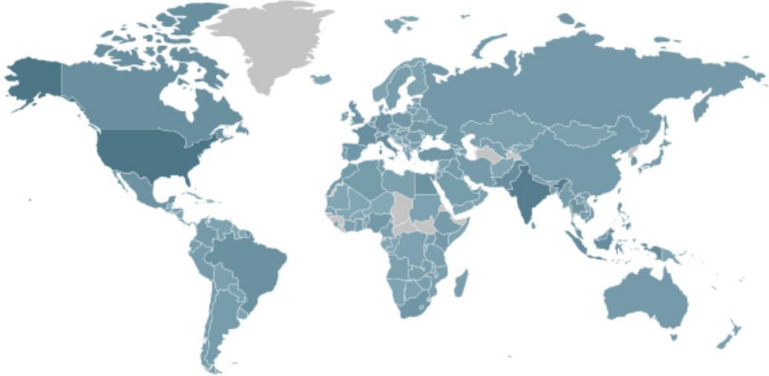
← → ↻ ⚠ Not secure

⋮

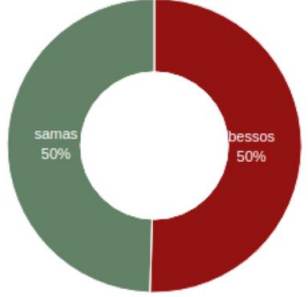
Geo Info

+

-



Frontends Use



bessos

samas

Active Projects

Id	Name	Bots: Online/Total/24h	Config	Status	
15	Boeing_white	2 / 257	77	Archive	Online Full Commands Notes Stats
21	British_white	2 / 438	77	Archive	Online Full Commands Notes Stats
30	Dassault_Arhive	161 / 1037	77	Archive	Online Full Commands Notes Stats
31	Socata_white	10 / 641	77	Archive	Online Full Commands Notes Stats
34	Kestrel_white	55 / 857	77	Archive	Online Full Commands Notes Stats
37	Embraer_white	42 / 452	77	Archive	Online Full Commands Notes Stats
43	Gulf_Arhive	66 / 610	77	Archive	Online Full Commands Notes Stats
44	Aerospace_white	11 / 190	77	Archive	Online Full Commands Notes Stats
47	Taygete_Garza_white	97 / 8171	77	Archive	Online Full Commands Notes Stats

UrlWatch Status

Group

Last for 24h

C2 Admin Panel

13

Anubis Panel [Bot With G x +

← → ↻ ⚠ Not secure

SmartAdmin SERVER TIME

ONLINE 1.0k BC BOTS 938 24H GROWTH 368 TOTAL 20.6k FAKES RBL [CLEAR]

Show Bot ex: 1.234543

Home / Dashboard / Bots / Grabbed Files

Bot With Grabberd Users Files

Botlist

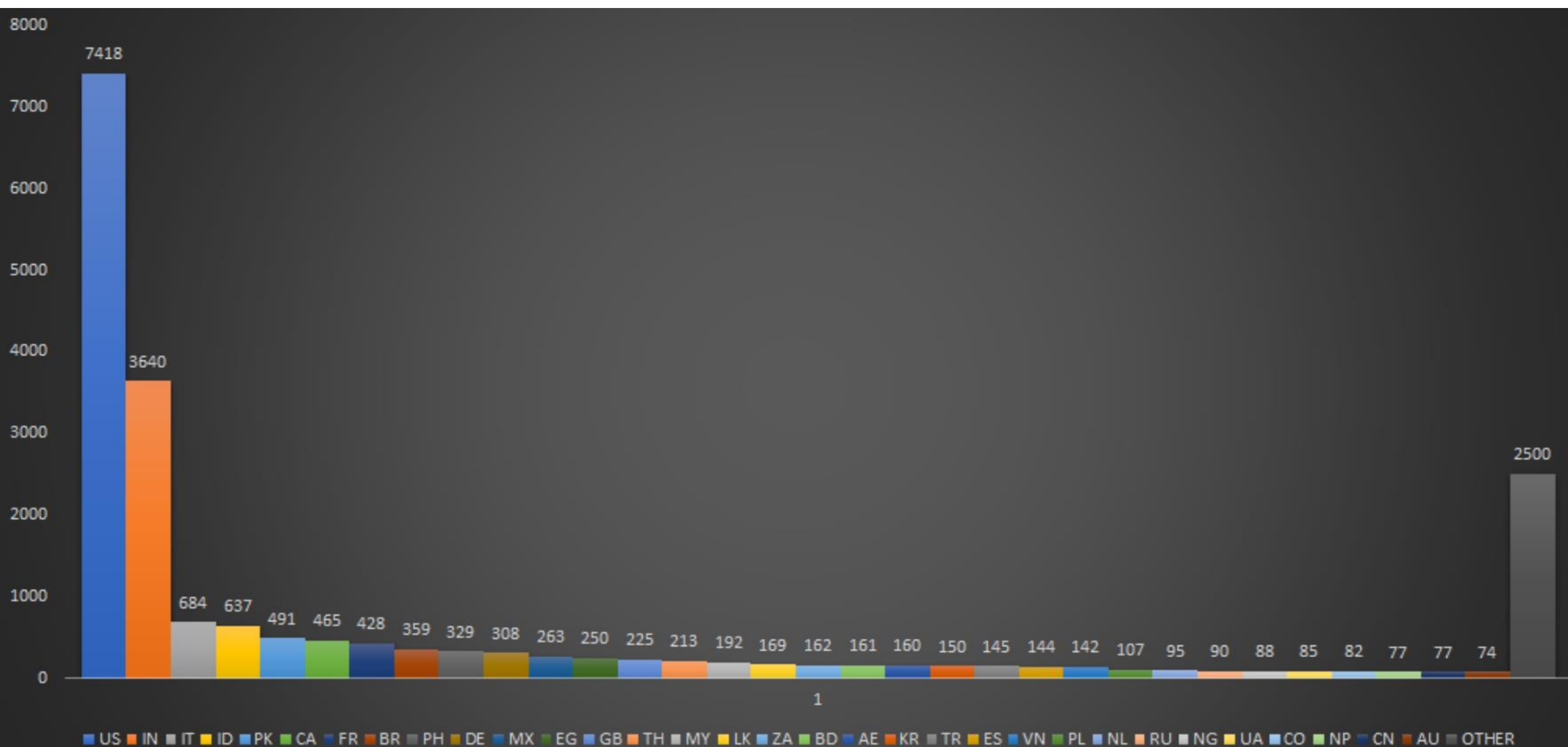
Project ID	Project Name	Bot ID	IP Address	First Time	Last Time	Is Online	Is BackConnect	Files
31	Socata_white	31.1044611288	228.166	2021-04-29 15:02:34	2021-09-17 13:27:31	Yes	Yes	C:\Users\Desktop\PASSWORD.txt
43	Gulf_Arhive	43.4240620214	146.114	2021-05-10 15:03:11	2021-08-10 02:25:01	No	No	c:\BIN\commands.log c:\DATA\HPMSG SVC.log c:\DATA\HPWMISVC.log c:\HPPU.log c:\HPQWare\BTBHost\Images\cpq_wc_logo.png c:\HPQWare\BTBHost\Images\hp_wc_logo.png c:\HPQWare\DropBox\HPAppDetector.log c:\Logs\DPTF.log c:\Logs\IntelChipset.log c:\Logs\IntelGFX.log c:\Logs\IntelGFXCoin.log c:\Logs\Intel\CCS.log c:\Logs\MBI.log c:\Common Files\McAfee\ClientAnalytics\Scripts\datasets_catalog.json c:\Common Files\McAfee\ClientAnalytics\Scripts\logging.js
11	Aerospatiale_Garza_white	11.3246787411	145.249	2021-05-09 22:22:19	2021-05-24 11:19:22	No	No	C:\Users\Desktop\Yusuf Binance.docx

Showing 1 to 3 of 3 entries

Previous 1 Next

Trojan Infection across the Globe

14



Do You Know ?

83% of all Critical Vulnerabilities published by Microsoft during the last 5 years can be mitigated by using a non-admin User Account



- 858 Microsoft Product Vulnerabilities were discovered in 2019
- Removing admin rights would mitigate 77% of all critical Microsoft vulnerabilities published in 2019
- 80% of Critical vulnerabilities in Windows Servers could be mitigated by using a non-admin user account.
- 100% of critical vulnerabilities in Internet Explorer could be mitigated by using a non-admin User account
- 80% of Critical Vulnerabilities in Windows 7, 8.1 and 10 could be mitigated by using a non-admin account



Keep your Operating System and Antivirus Updated with latest Patches/Updates



Create a non-admin account in your OS/ System and Use it for day to day activities



Don't use any Pirated Softwares or Cracks or Keygens.



Disable Powershell and Remote Desktop

Report Security Incident to NIC-CERT :



011-22902400



incident@nic-cert.nic.in



<https://nic-cert.nic.in>

Security Checklist

1. **Firmware, OS, Softwares & Antivirus** – Updated with **Latest updates + Patches**
2. **Use non-admin User account for day to day activities**
3. **Disable Powershell and Remote Desktop**
4. **Install Apps from official App Stores** of OEMs & Don't root/jailbreak your Phones
5. Don't use any illegal/pirated software, cracks, keygen..etc
6. **Use Multi-Factor Authentication** for your accounts & Don't re-use passwords
7. **Maintain Offline backup of Critical data**
8. **Don't Click on any Urls, Shortened links**, without proper verification
9. **Don't Open any mail attachments / shared or downloaded files without scanning it with AntiVirus**
10. Avoid installing any unnecessary browser plugins, toolbars...etc

How can a simple Search Lead to a cyber attack

17



Write a resume and cover letter + pdf



All



News



Images



Videos



Maps



More

Tools

Page 8 of about 6,90,00,000 results (0.63 seconds)

<https://www.coolfreecv.com> › cover-letter-builder ▾

Cover Letter Examples - Free Maker Creator Builder Online PDF

Not sure what to **write**? Our experts have written this section for you. **Create** a tailored **Cover Letter** for each job position you want to apply for. Privacy ...

<https://www.myp perfect resume.com> › cover-letter › tem... ▾

12+ Professional Cover Letter Templates for Your Resume

Choose a **cover letter** template, follow our step by step guide to add your info, and in minutes you'll **write** a **cover letter** that gets interviews!

★★★★★ Rating: 4.8 · 818 votes

<https://www.jobscan.co> › cover-letter-formats ▾

Cover Letter Formats: Choosing the Best Type of ... - Jobscan

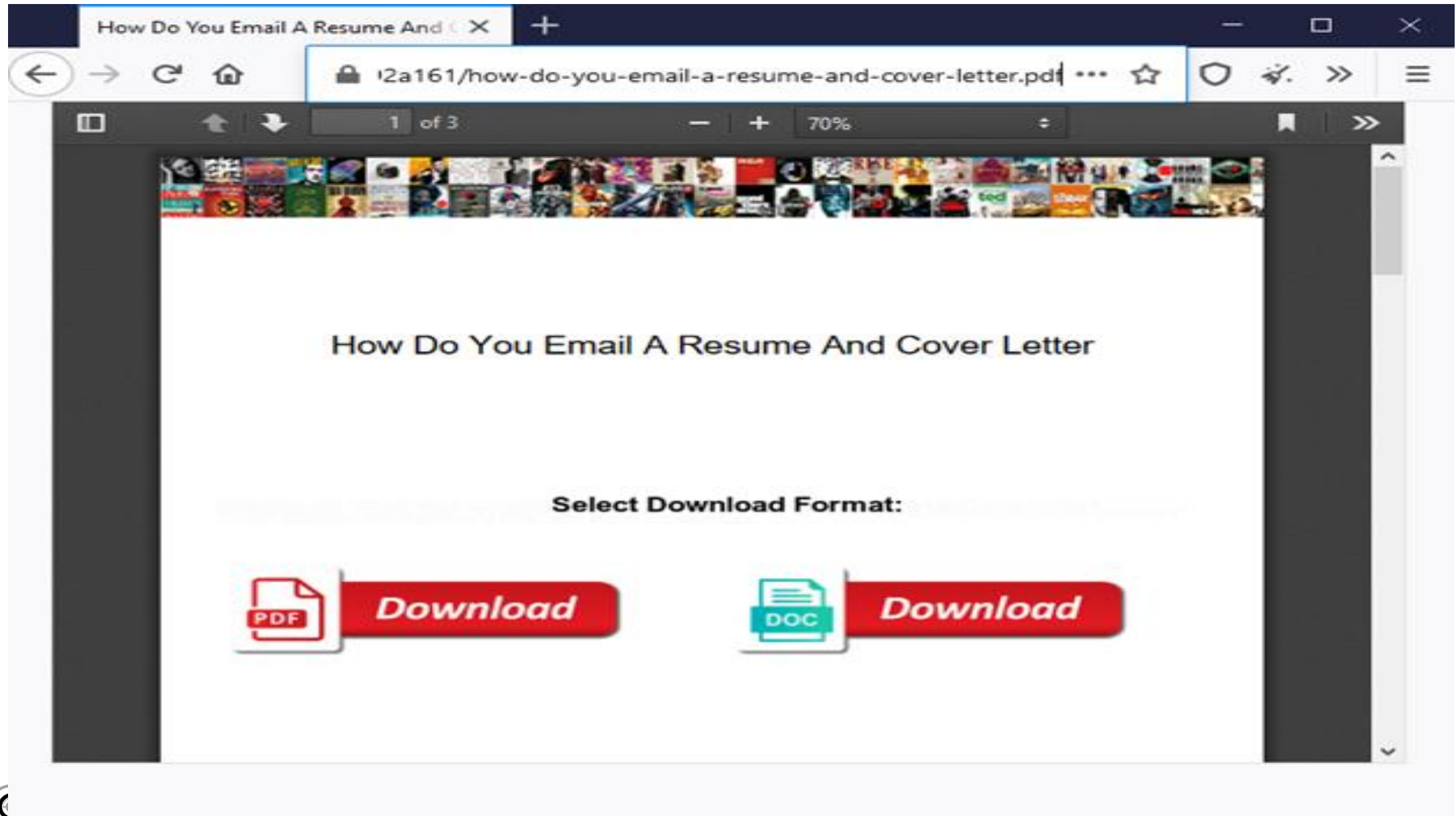
This is the standard **cover letter** used alongside a **resume** during a job application. The **application letter** is geared toward a certain job, and it is tailored to ...

<https://students.wustl.edu> › resumes-cover-letters ▾

Resumes and Cover Letters - Students - Washington ...

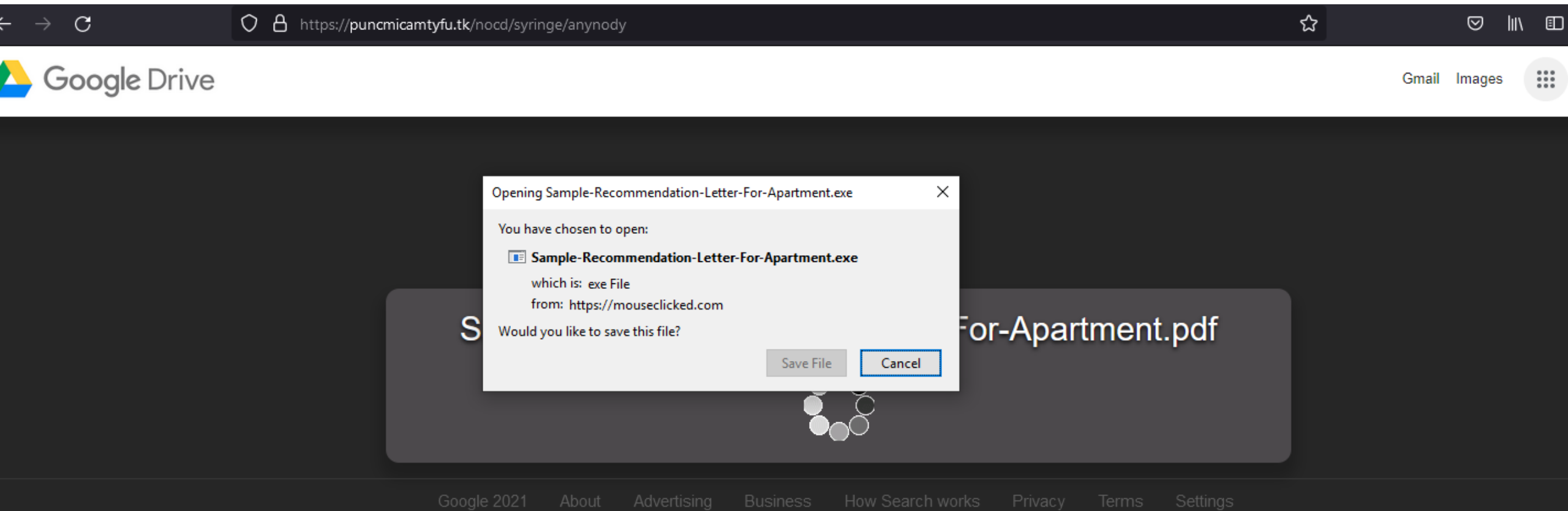
Refer to this **Resume and Cover Letter** handout(PDF) to learn how to **make** a great first impression. This handout covers: **resume** tips, **resume** formatting, tailoring ...

Trojanised PDFs



Hackers targeting keywords and SEO

19



Browser Plugins injecting Ads

20

The screenshot shows a Google search for "ipad". The search bar at the top contains the word "ipad" and a magnifying glass icon. Below the search bar, there are tabs for "Web", "Images", "News", "Videos", "More", and "Search tools". The "Web" tab is selected. The search results show "About 829,000,000 results (0.44 seconds)".

The first search result is "Apple iPad - Every Day Low Prices at Walmart - walmart.ca". It includes a Walmart logo, the URL "www.walmart.ca/Apple-iPad", and text about free shipping and ratings. Below this are two columns of text: "Electronics on Clearance" and "Top Rated Electronics" on the left, and "Electronics on Rollback" and "Discover Walmart.ca" on the right.

The second search result is "iPad Air 2 - Apple Store". It includes an Apple logo, the URL "store.apple.com/iPad", and text about the iPad Air 2 being available in Gold, Silver, and Space Gray, with a price starting at \$549. It also mentions the location "100 City Centre Dr, Mississauga, ON" and a phone number "(905) 366-0580".

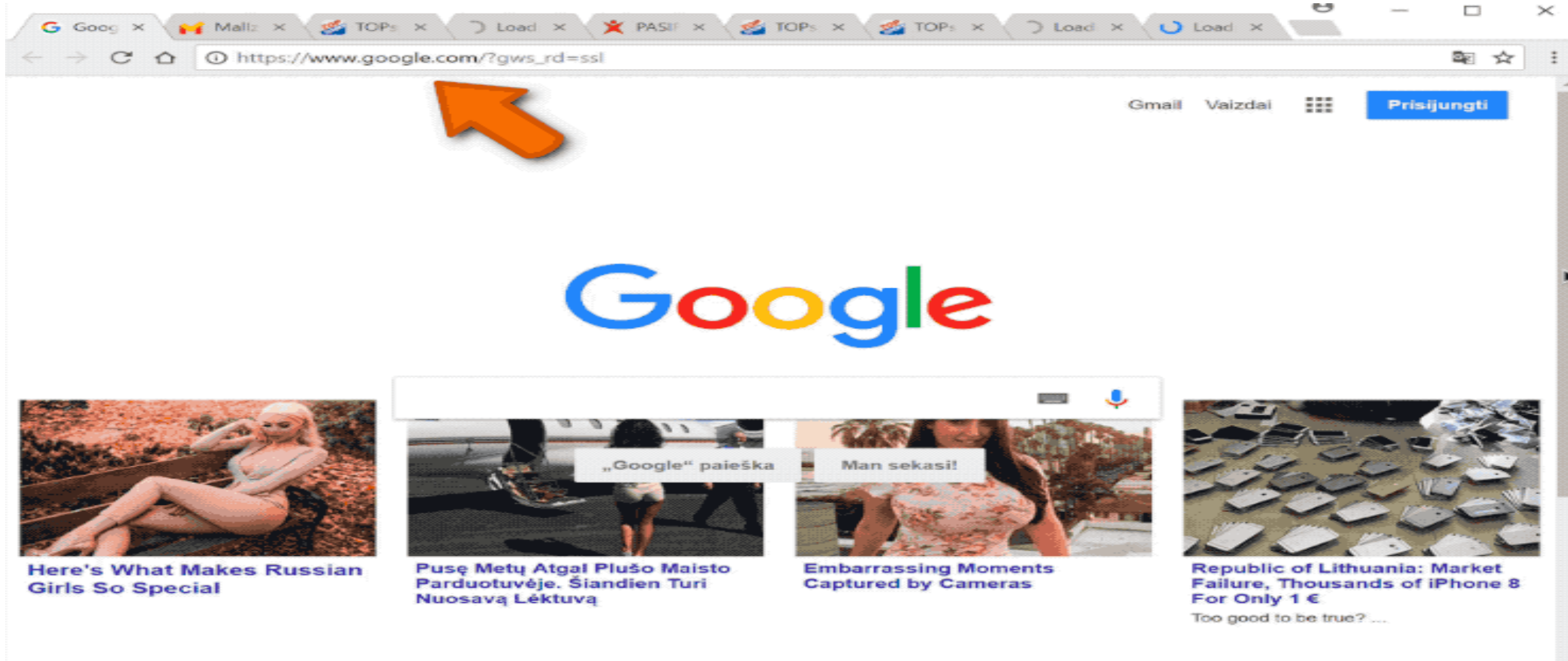
The third search result is "iPad at Bell - bell.ca". It includes a Bell logo, the URL "www.bell.ca/iPad", and text about getting connected to Canada's largest LTE network. It also mentions "Bell Canada has 3,641 followers on Google+" and links to "Compare iPads", "Find a Bell store", "iPad rate plans", and "iPad for business".

On the right side of the search results, there are several sponsored ads. The first is "iPad at Amazon" with the URL "www.amazon.ca/iPad" and text about saving big on new gear and free 2-day shipping with Amazon Prime. The second is "iPad on Kijiji" with the URL "www.kijiji.ca/Phones-Tablets" and text about browsing photos, prices, and more on Kijiji. The third is "Apple iPads up to 75% off" with the URL "ca.sale-fire.com/Apple+iPads" and text about an Apple iPad sale and free shipping. The fourth is "Top 10 iPad Tablets 2014" with the URL "www.comparison411.com/iPad" and text about cheap prices on all iPad tablets. The fifth is "iPad 5" with the URL "www.ebay.ca/" and text about getting an iPad 5 on eBay and the new eBay Buyer Protection Program. At the bottom of the ads is a link "See your ad here >".

At the bottom of the search results, there is a "Visual Search results" section. It is titled "Visual Search results" and "Powered by browsers+apps+1.1 [x]". It contains two product images: an "Apple iPad 2 16GB Black" priced at "\$299.99" from "Toys R Us", and an "Apple iPad Air 32GB Silver" priced at "\$499.99" from "Toys R Us". A large orange arrow points from the right towards the Visual Search section.

Browser Plugins injecting Ads

21



MoD : Case Study

22



禪

Ministry of Defence

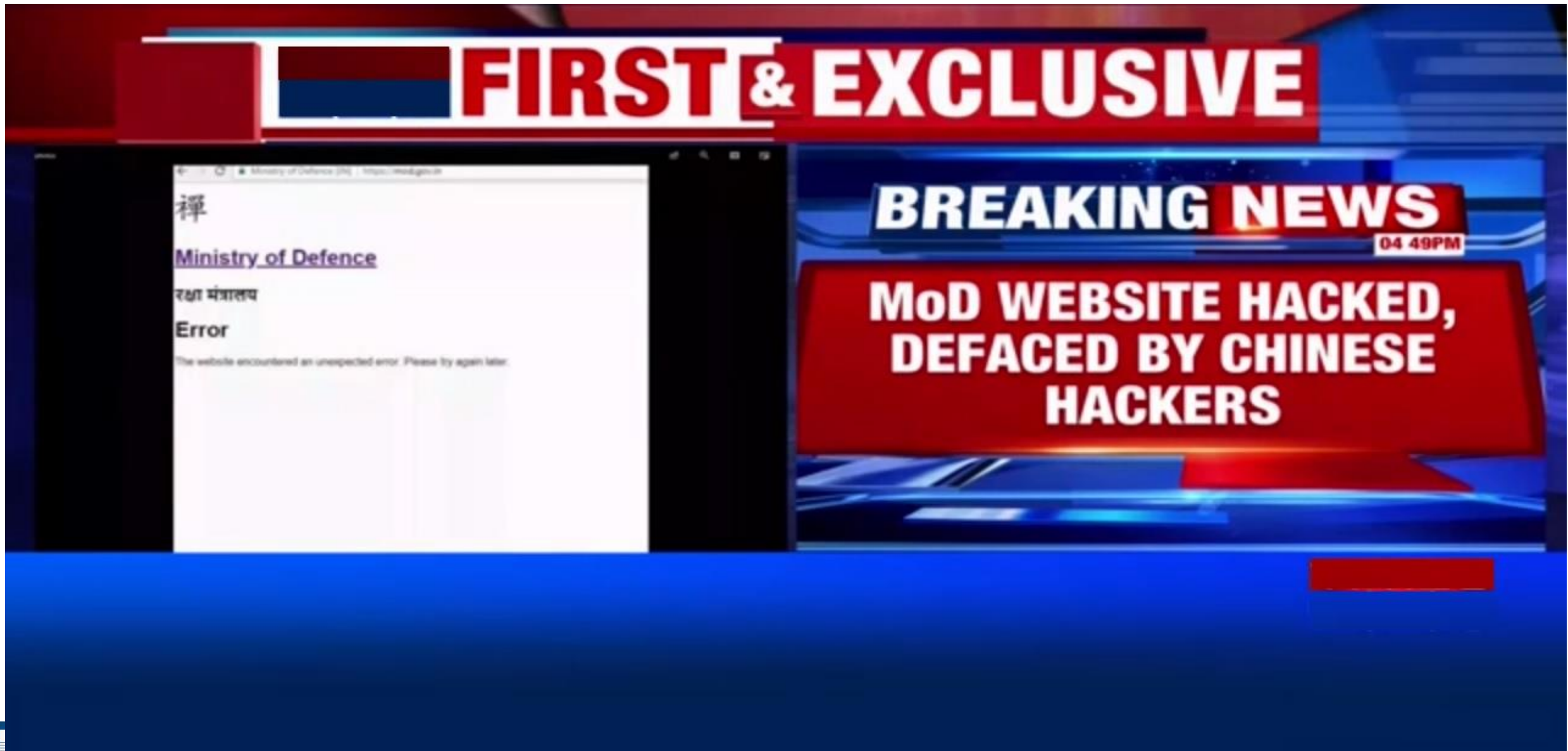
रक्षा मंत्रालय

Error

The website encountered an unexpected error. Please try again later.

MoD : Media Coverage

23



MoD : Media Coverage

24



MoD case on twitter



Nirmala Sitharaman ✓

@nsitharaman

Follow

Action is initiated after the hacking of MoD website (mod.nic.in). The website shall be restored shortly. Needless to say, every possible step required to prevent any such eventuality in the future will be taken.

[@DefenceMinIndia](#) [@PIB_India](#) [@PIBHindi](#)

4:46 AM - 6 Apr 2018

452 Retweets 1,271 Likes



239



452



1.3K



Kovid Raj ⚡ @KovidRaj5 · 6 Apr 2018

Replying to [@nsitharaman](#) [@DefenceMinIndia](#) and 2 others

Ur Govt cant even defend a website and how will u defend the Borders...?

[#IndiaDoesNotTrustBJP](#)



6



11



49

Tweet unavailable

MoD case on twitter

26



NIC ✓
@NICMeity

Follow

mod.gov.in is NOT HACKED. There is some technical issue since 2:30PM today. Drupal theme drupal.org/project/zen framework. The site displayed the default logo.

@drajaykumar_ias @nsitharaman

@DefenceMinIndia @PIB_India @PIBHindi



Zen

Zen is a modern, powerful, HTML5 starting theme with component-based CSS and a responsive, mobile-first grid design. If you are building your own standards-compliant theme, you wi...

drupal.org

5:54 AM - 6 Apr 2018

97 Retweets 87 Likes



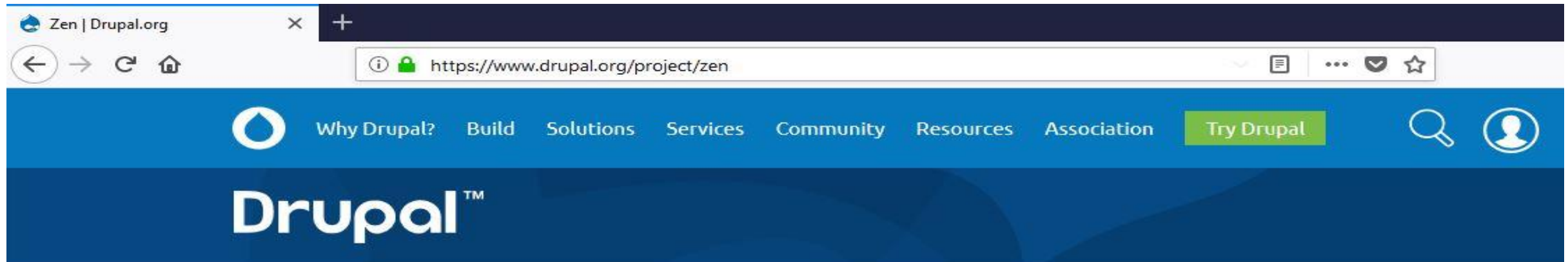
10

97

87

Root Cause of MoD Issue

27



Download & Extend

[Drupal Core](#) [Distributions](#) [Modules](#) [Themes](#)

Zen

[View](#) [Version control](#) [Automated testing](#)

Posted by [JohnAlbin](#) on 11 October 2006, updated 7 December 2017

Zen is a modern, powerful, HTML5 starting theme with component-based CSS and a responsive, mobile-first grid design. If you are building your own standards-compliant theme, you will find it much easier to start with Zen than to start with Bartik or Stark. This theme has [fantastic online documentation](#) and tons of helpful code comments in its JavaScript, PHP, HTML, CSS and Sass.



★ 17

Maintainers for Zen

[JohnAlbin](#) - 2039 commits
last: 7 months ago, first: 10 years ago

[echoz](#) - 26 commits
last: 4 years ago, first: 6 years ago

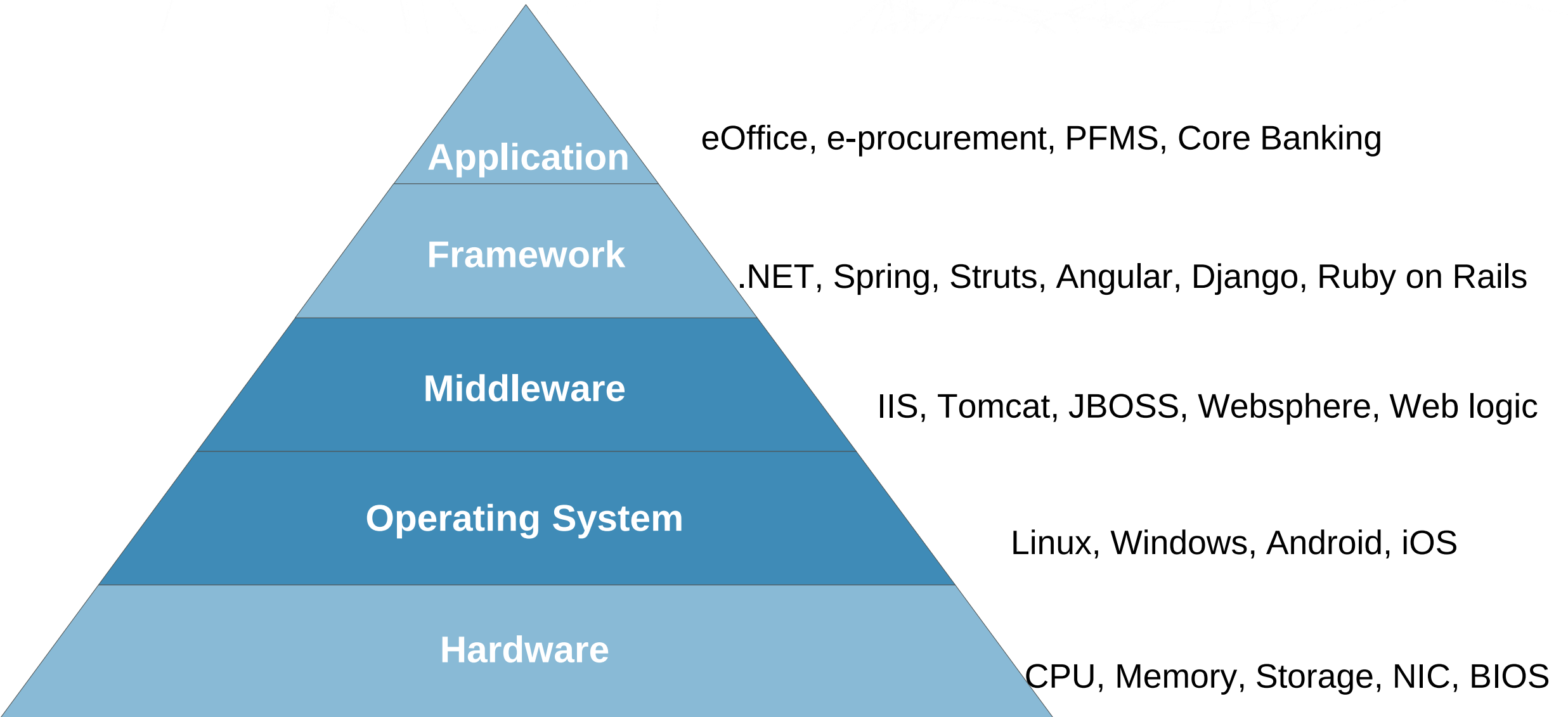
[View all committers](#)

[View commits](#)

Zen now comes with modern front-end development practices!

[HTML5](#) [RTL](#) [Mobile-first](#) [Components](#) [Style guide](#) [Task runner](#)

Application + IT Infrastructure Components



Have You Seen this?



3 Angry Cats
=
Thrangrycat

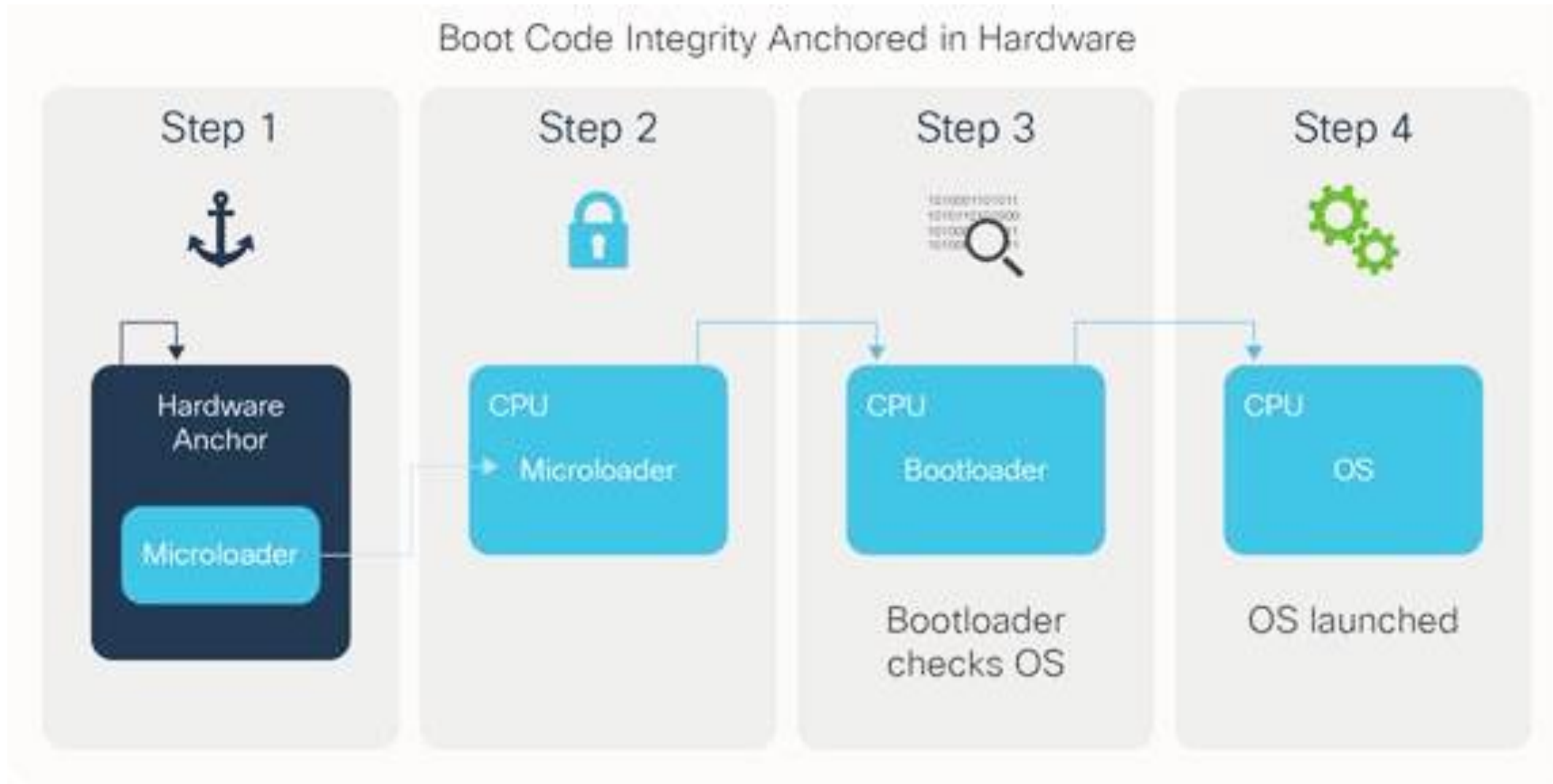
OH, WE'RE A SECURITY THREAT NOW?



GOOD

Cisco Secure Boot

32



Emerging Cyber Risks

What do you See?

34

adobe.com

apple.com

bankofamerica.com

cisco.com

ebay.com

facebook.com

google.com

microsoft.com

netflix.com

poloniex.com

twitter.com

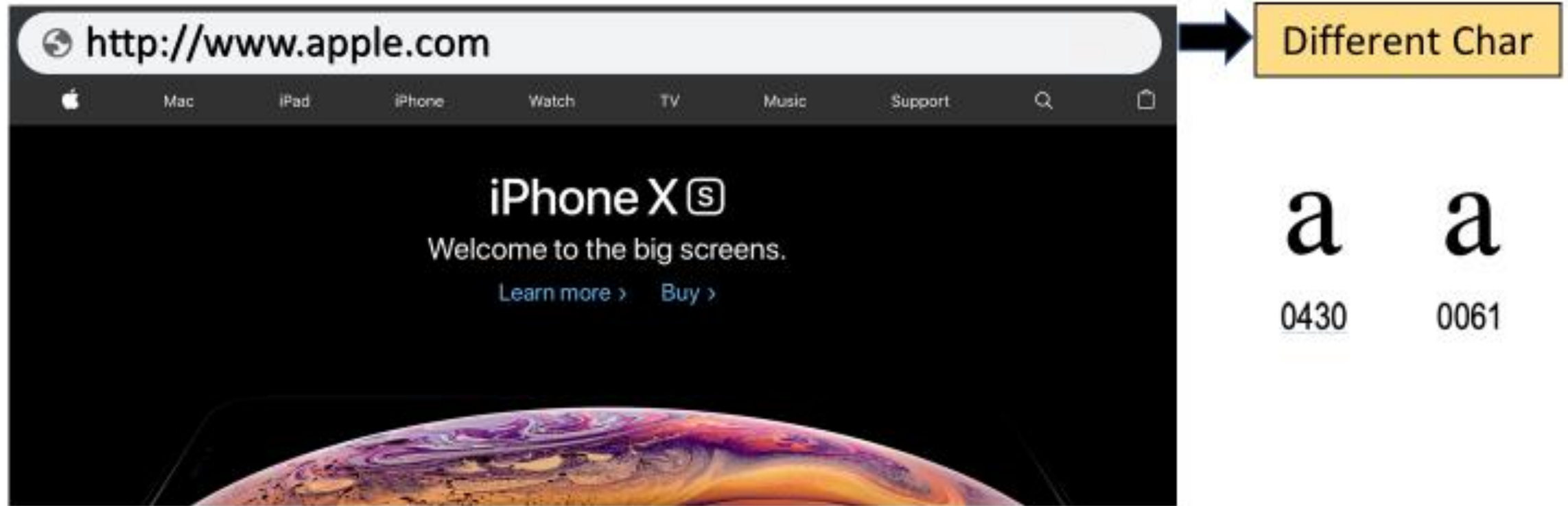
wellsfargo.com

wikipedia.com

Apple.com



Apple.com



- This is IDN (Internalized Domain Name) homograph attack
- Homograph domain squatting: Exploit the fact that many different characters look alike

facebook

 <https://www.facebook.com>

facebook

Email or phone

Password

Log In

Forgot account?

Connect with friends and the world around you on Facebook.



See photos and updates from friends in News Feed.



Share what's new in your life on your Timeline.



Find more of what you're looking for with Facebook Search.

Sign Up

It's free and always will be.

First name

Last name

Mobile number or email

New password

Birthday

Jan 10 1990

Why do I need to provide my birthday?

☐ Female

☐ Male

By clicking Create Account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use. You may receive SMS notifications from Facebook and can opt out at any time.

Create Account

Create a Page for a celebrity, band or business.

English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 日本語 Deutsch 한국어 日本語 +

Sign Up

Log In

Messenger

Facebook Lite

Mobile

Find Friends

People

Pages

Places

Games

Locations

Celebrities

Marketplace

Groups

Reels

Sports

Look

Moments

Instagram

Local

About

Create Ad

Create Page

Developers

Careers

Privacy

Cookies

Ad Choices

Terms

Help

Facebook © 2018

Adobe Flashplayer

https://get.adobe.com/en/flashplayer

Adobe Flash Player

Acerca de:
Adobe® Flash® Player es un

Términos y condiciones:
Haciendo clic en el botón "Instalar ahora", reconoce haber leído y aceptar [Acuerdo de licencia de software de Adobe](#).

Nota: Adobe Flash Player es una aplicación integrada, pero se puede desactivar. Haga clic aquí para solucionar problemas de reproducción de Flash Player.

Opening flashplayer27_pp_xa_install.exe

You have chosen to open:

 **flashplayer27_pp_xa_install.exe**
which is: Binary File
from: http://get.adobe.com

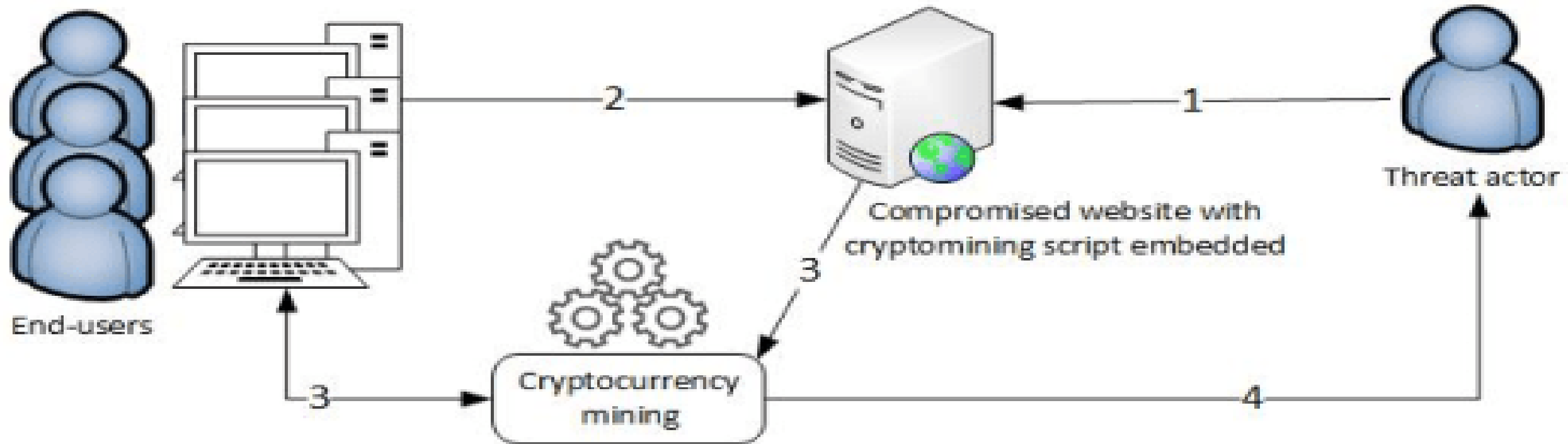
Would you like to save this file?

Save File Cancel

Cryptojacking

Cryptojacking

40



41





Thank You

incident@nic-cert.nic.in
(+91)011 22902400