End-User Guide

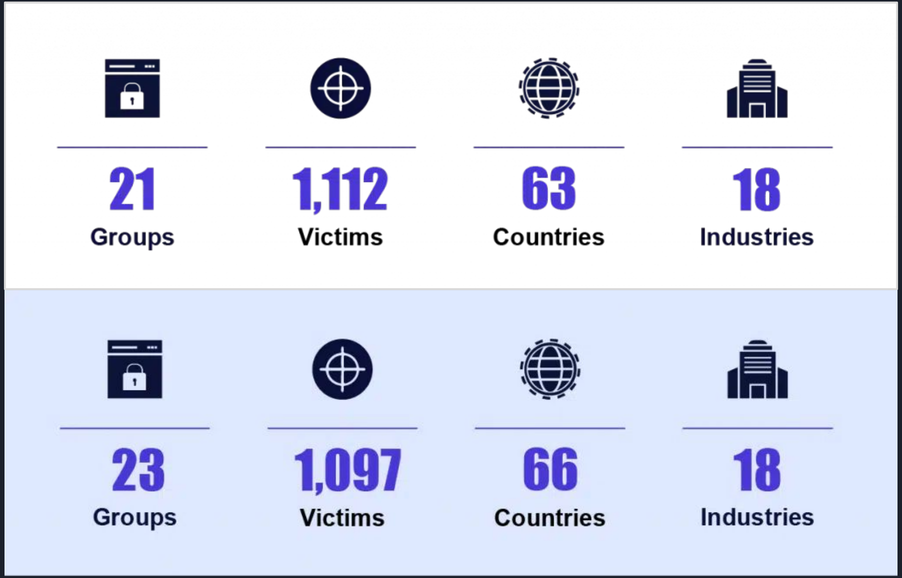
Tao Zimmerman, Colton Hulce,
Louis Najdek, William Atwood

Information Disclaimer

The testing performed was done in a safe environment, with no connection to any network. We are not responsible for any damages caused by attempting the content depicted in this presentation.

Introduction

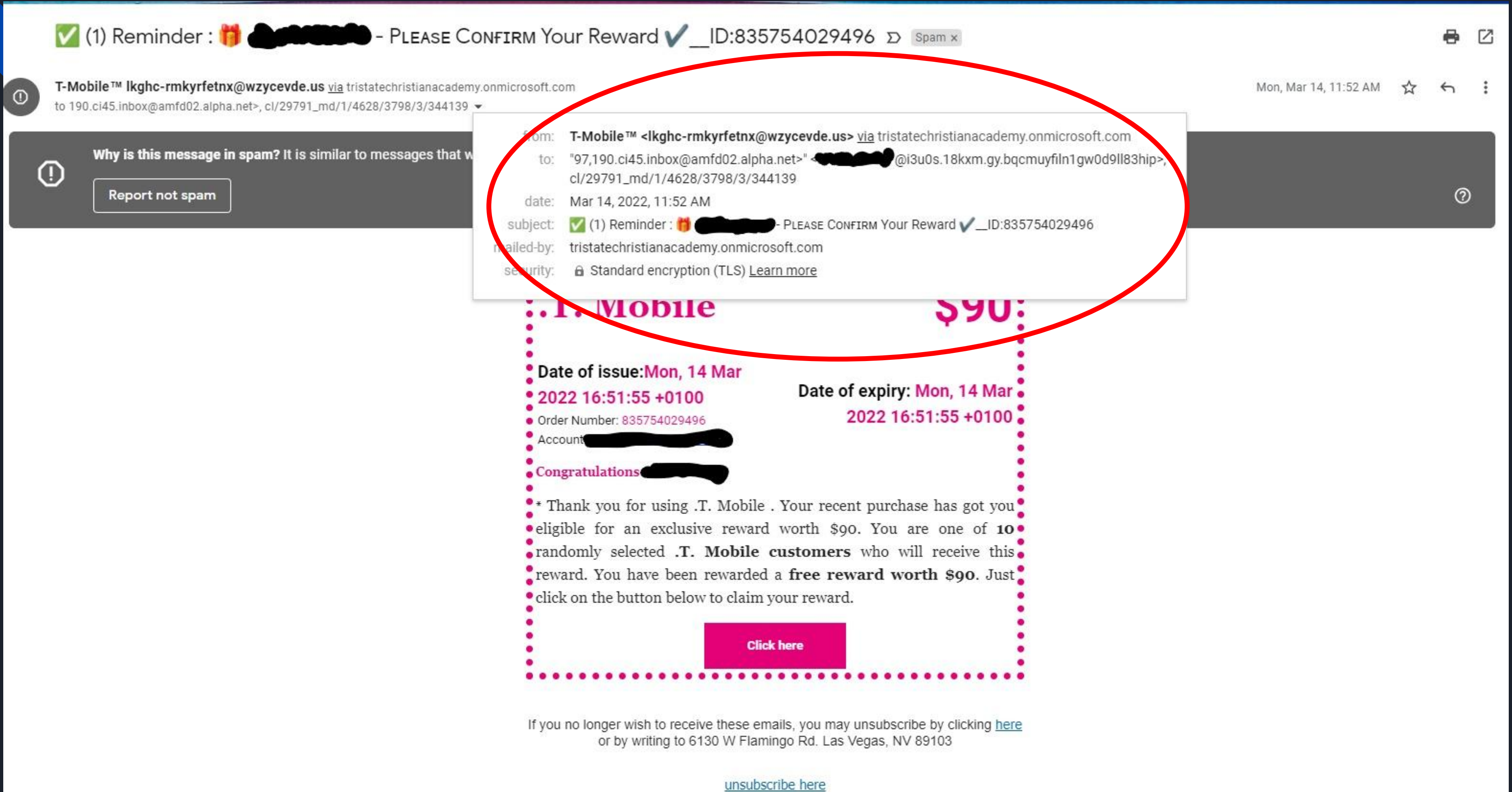
- "In 2020, 1,112 organizations were hit by ransomware attacks. In comparison, 1,097 organizations were hit by ransomware attacks in the first **half** of 2021."



21 Groups	1,112 Victims	63 Countries	18 Industries
23 Groups	1,097 Victims	66 Countries	18 Industries

Source: https://www.cognyte.com/blog/ransomware_2021/

Attack Vectors - Phishing Emails



✅ (1) Reminder : 🎁 [redacted] - PLEASE CONFIRM Your Reward ✔__ID:835754029496 Spam ×

T-Mobile™ lkghc-rmkyrfetnx@wzycevde.us via tristatechristianacademy.onmicrosoft.com
to 190.ci45.inbox@amfd02.alpha.net>, cl/29791_md/1/4628/3798/3/344139

Mon, Mar 14, 11:52 AM

Why is this message in spam? It is similar to messages that w

Report not spam

from: T-Mobile™ <lkghc-rmkyrfetnx@wzycevde.us> via tristatechristianacademy.onmicrosoft.com
to: "97,190.ci45.inbox@amfd02.alpha.net>" <[redacted]@i3u0s.18kxm.gy.bqcmuyfiln1gw0d9ll83hip>, cl/29791_md/1/4628/3798/3/344139
date: Mar 14, 2022, 11:52 AM
subject: ✅ (1) Reminder : 🎁 [redacted] - PLEASE CONFIRM Your Reward ✔__ID:835754029496
mailed-by: tristatechristianacademy.onmicrosoft.com
security: 🔒 Standard encryption (TLS) Learn more

.T. Mobile $90!

Date of issue: Mon, 14 Mar 2022 16:51:55 +0100

Date of expiry: Mon, 14 Mar 2022 16:51:55 +0100

Order Number: 835754029496
Account [redacted]

Congratulations [redacted]

* Thank you for using .T. Mobile . Your recent purchase has got you eligible for an exclusive reward worth $90. You are one of **10** randomly selected **.T. Mobile customers** who will receive this reward. You have been rewarded a **free reward worth $90**. Just click on the button below to claim your reward.

Click here

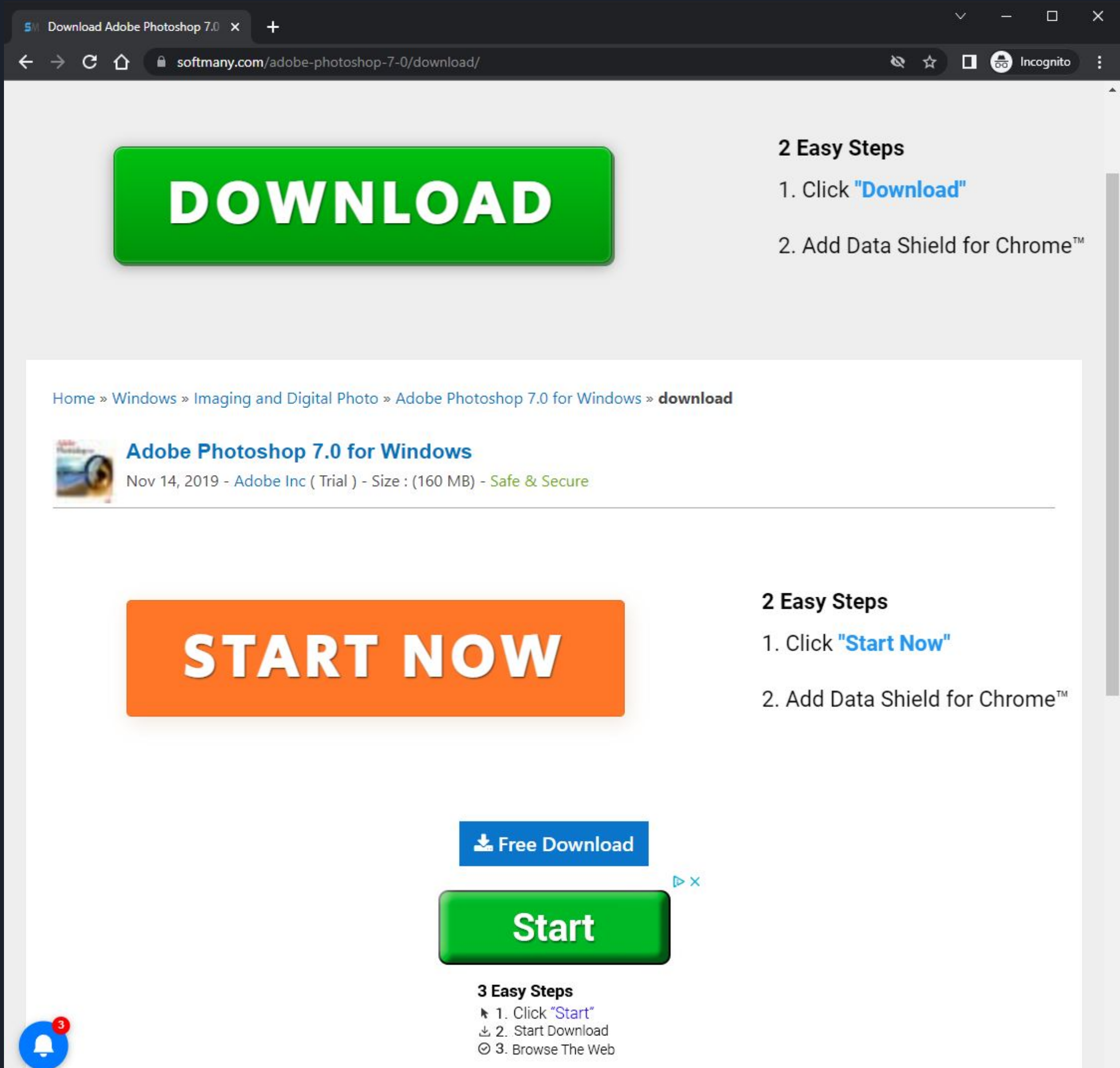
If you no longer wish to receive these emails, you may unsubscribe by clicking here
or by writing to 6130 W Flamingo Rd. Las Vegas, NV 89103

unsubscribe here

Attack Vectors - Downloads

Note:

- The unofficial URL
- The suggestion to download 'data shield' for chrome.
- Not a single word is said otherwise, it just wants you to download data shield. Which is most likely bad for you.
- The fake "download" and "start" buttons


Download Adobe Photoshop 7.0
softmany.com/adobe-photoshop-7-0/download/
Incognito
DOWNLOAD
START NOW
Free Download
Start
3

2 Easy Steps

1. Click "Download"

2. Add Data Shield for Chrome™

Home » Windows » Imaging and Digital Photo » Adobe Photoshop 7.0 for Windows » **download**

Adobe Photoshop 7.0 for Windows

Nov 14, 2019 - Adobe Inc (Trial) - Size : (160 MB) - Safe & Secure

2 Easy Steps

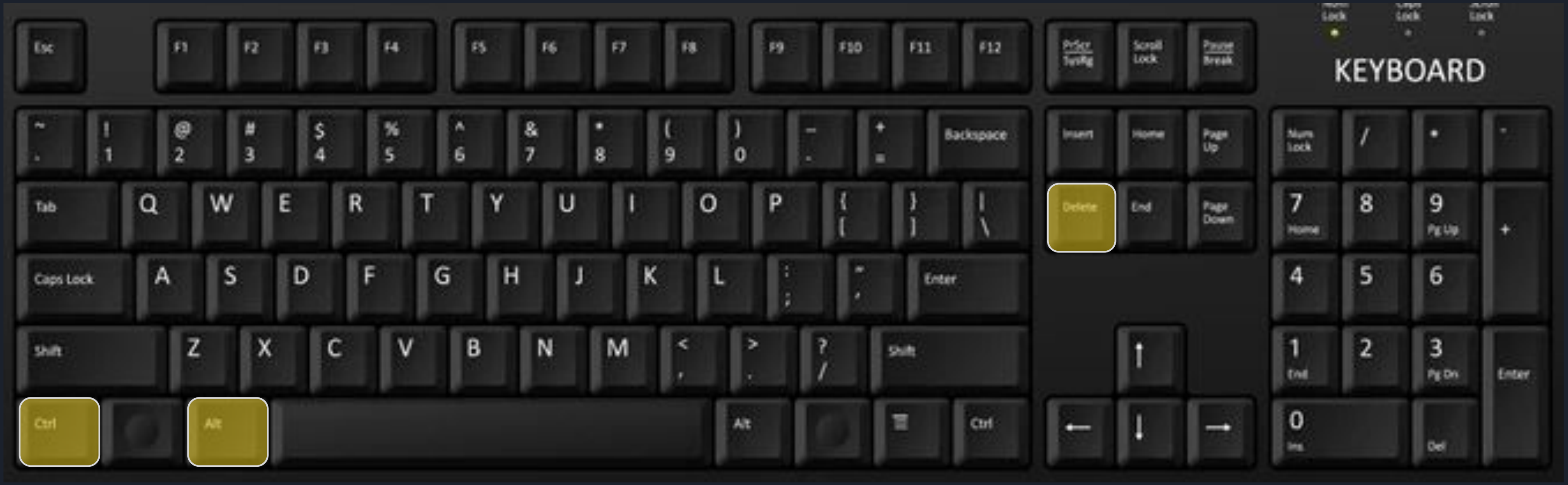
1. Click "Start Now"

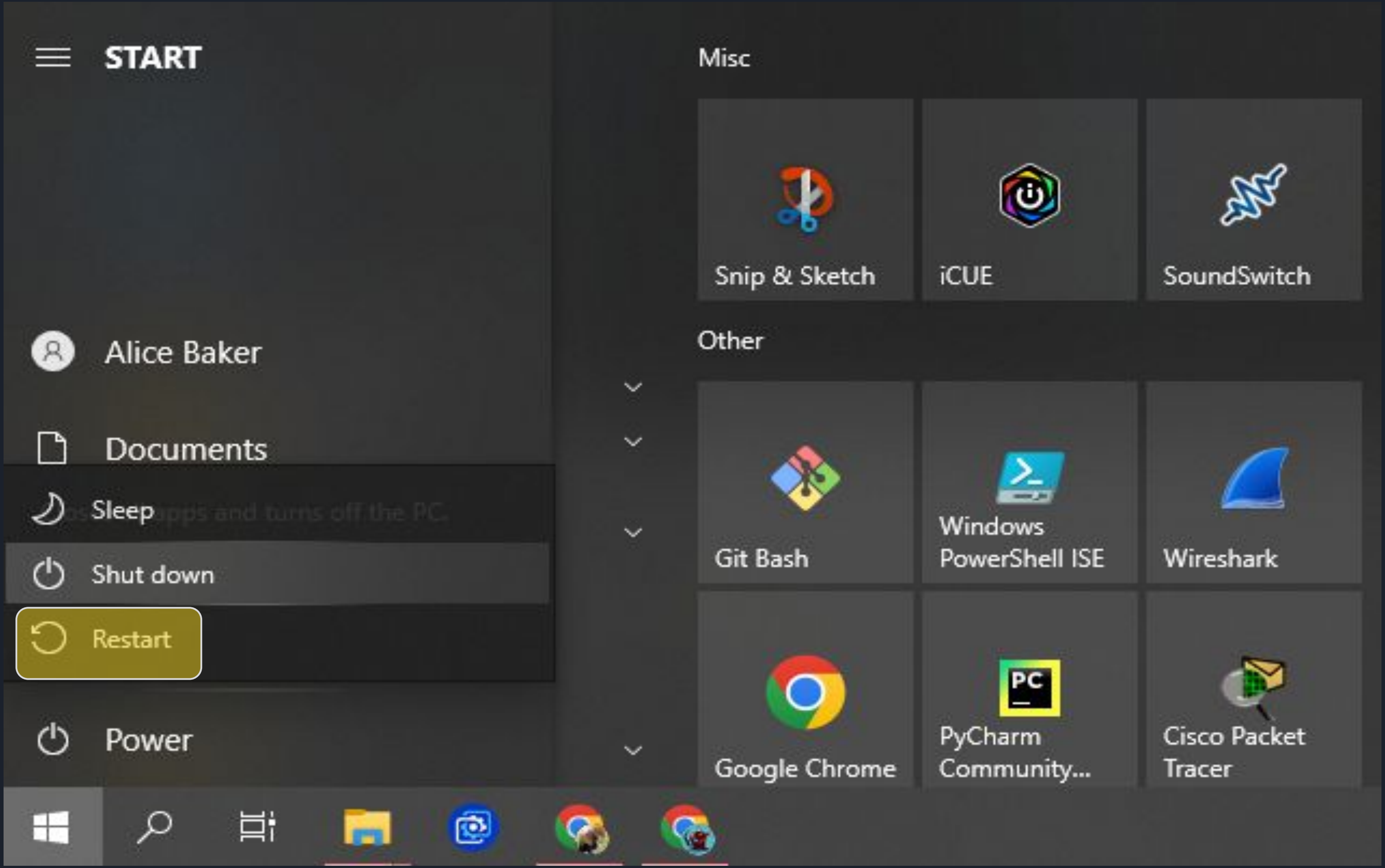
2. Add Data Shield for Chrome™

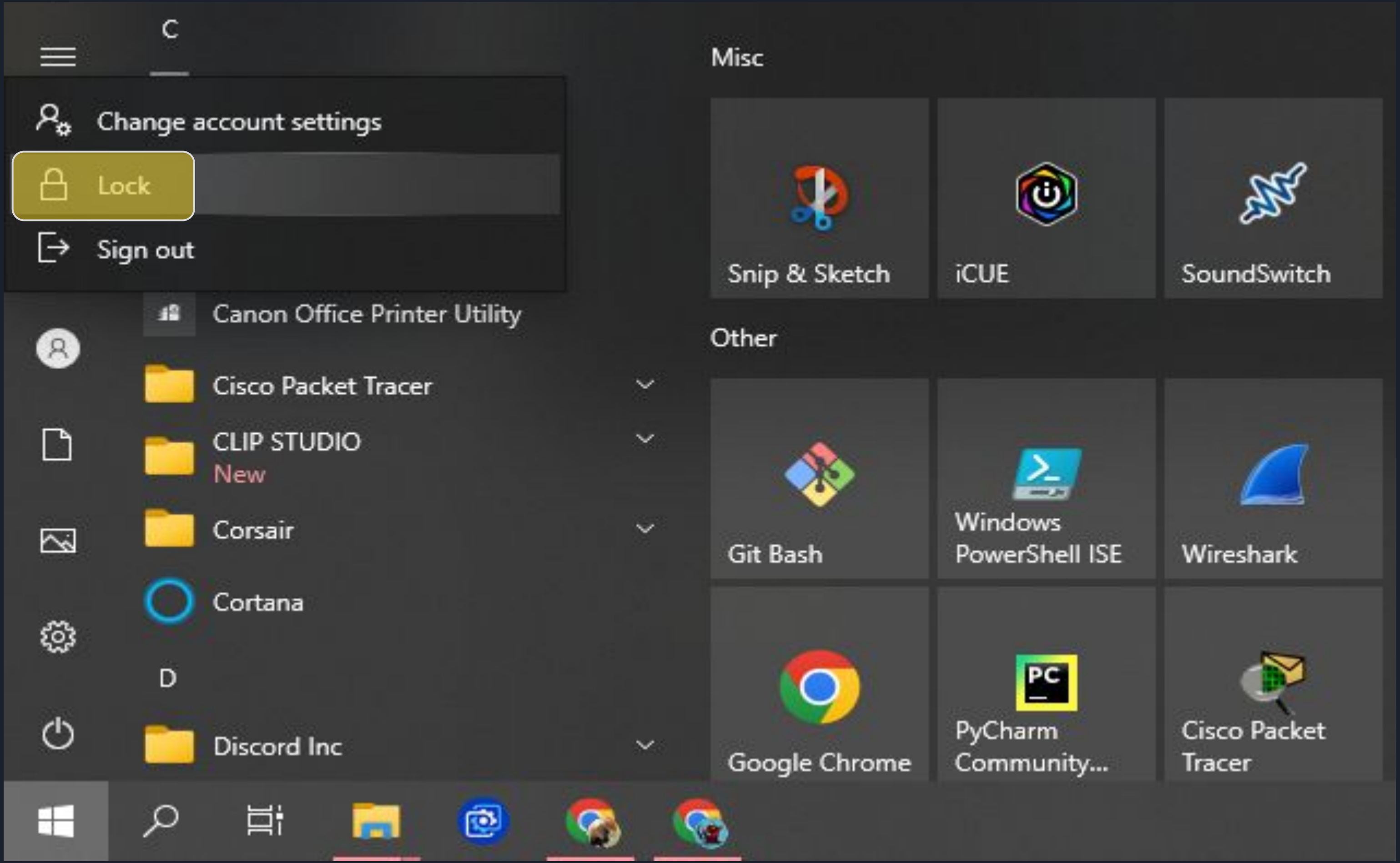
3 Easy Steps

1. Click "Start"
2. Start Download
3. Browse The Web

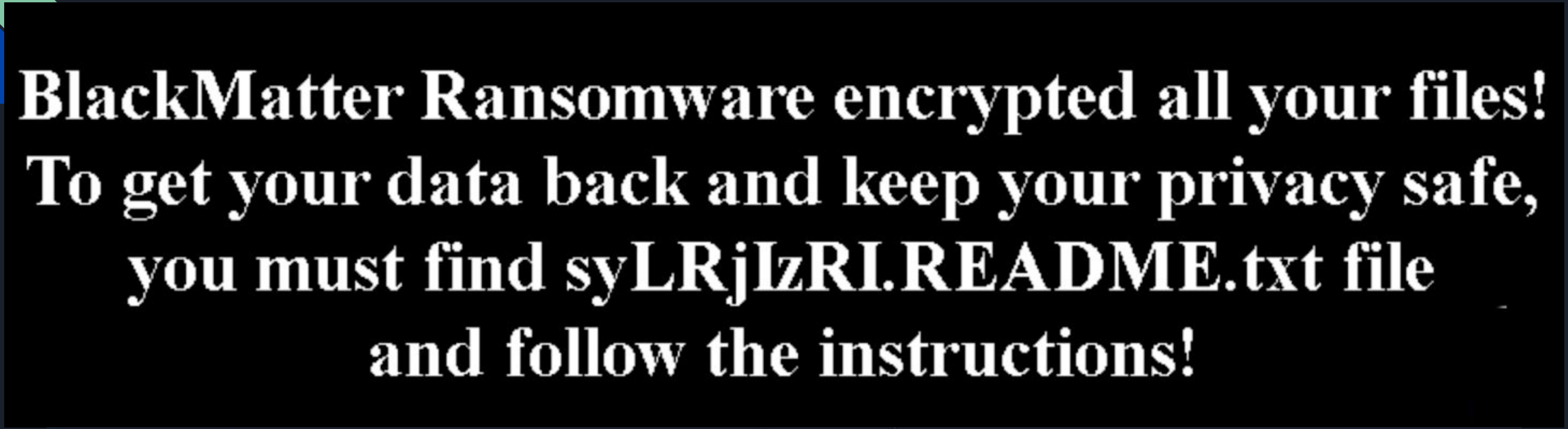
Internal Attacks



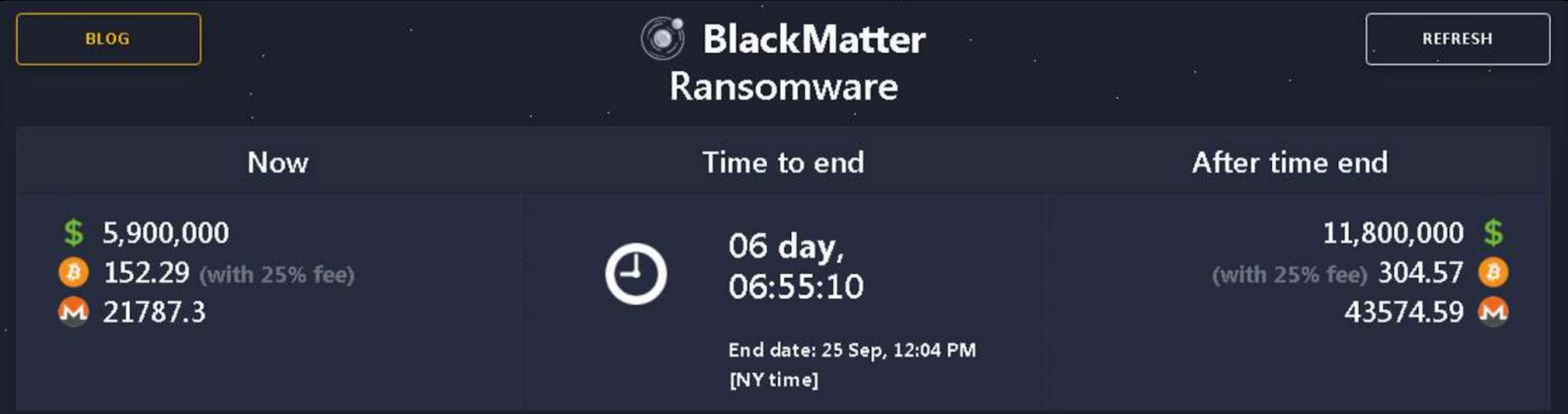

START
Alice Baker
Documents
Sleep
apps and turns off the PC.
Shut down
Restart
Power
Misc
Snip & Sketch
iCUE
SoundSwitch
Other
Git Bash
Windows PowerShell ISE
Wireshark
Google Chrome
PyCharm Community...
Cisco Packet Tracer


C
Change account settings
Lock
Sign out
Canon Office Printer Utility
Cisco Packet Tracer
CLIP STUDIO
New
Corsair
Cortana
D
Discord Inc
Misc
Snip & Sketch
iCUE
SoundSwitch
Other
Git Bash
Windows PowerShell ISE
Wireshark
Google Chrome
PyCharm Community...
Cisco Packet Tracer

Indicators of Compromise



BlackMatter Ransomware encrypted all your files!
To get your data back and keep your privacy safe,
you must find syLRjIzRI.README.txt file
and follow the instructions!



Now	Time to end	After time end
$ 5,900,000 ₿ 152.29 (with 25% fee) M 21787.3	06 day, 06:55:10 End date: 25 Sep, 12:04 PM [NY time]	11,800,000 $ (with 25% fee) 304.57 ₿ 43574.59 M

Sources

Introduction -

- “Ransomware Attack Statistics 2021 - Growth & Analysis”. Cognyte. Cognyte. 08 Aug 2021. https://www.cognyte.com/blog/ransomware_2021/

Indicators of Compromise -

- Ozarslan, Suleyman. “BlackMatter Ransomware Analysis, TTPs and IOCs”. Picus Labs. Picus Security. 21 Oct 2021. https://www.picussecurity.com/resource/blog/blackmatter-ransomware-analysis-ttps-and-iocs