The Evolution of Ransomware

From Floppies to Droppers

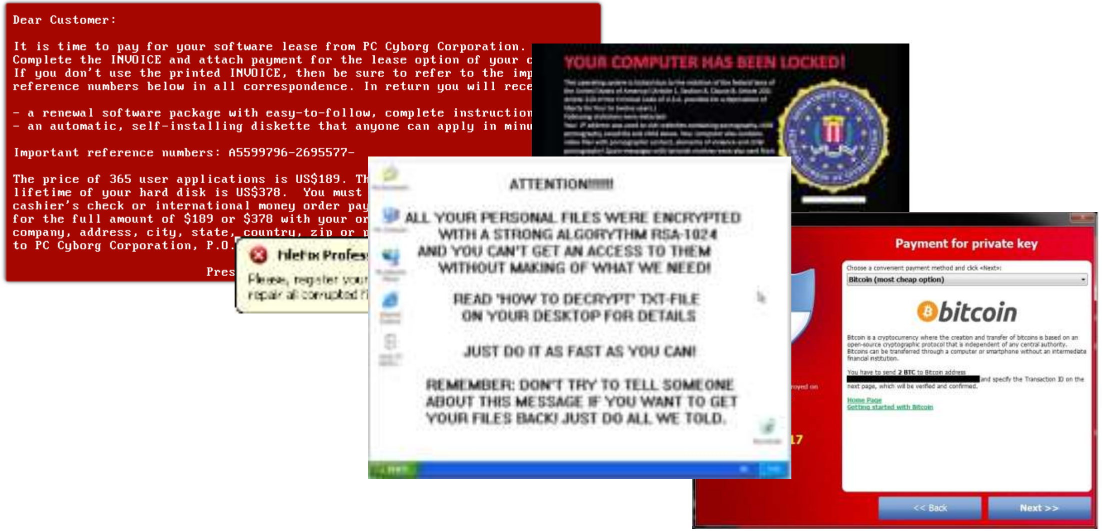
Eliad Kimhy
Head of ASR CORE team

Story Time

- First Ransomware
- Evolution
- What changed?
- What can we learn?
- How can we address it?

What was the First Ransomware Incident?

- 2006
- 1989
- 1996
- 2013



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your c
If you don't use the printed INVOICE, then be sure to refer to the imp
reference numbers below in all correspondence. In return you will rece

- a renewal software package with easy-to-follow, complete instruction
- an automatic, self-installing diskette that anyone can apply in minu

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. Th
lifetime of your hard disk is US$378.  You must
cashier's check or international money order pay
for the full amount of $189 or $378 with your or
company, address, city, state, country, zip or p
to PC Cyborg Corporation, P.O.

                          Pres
```

Filefix Profess

Please, register your
repair all corrupted fi

YOUR COMPUTER HAS BEEN LOCKED!

ATTENTION!!!!!!

ALL YOUR PERSONAL FILES WERE ENCRYPTED
WITH A STRONG ALGORYTHM RSA-1024
AND YOU CAN'T GET AN ACCESS TO THEM
WITHOUT MAKING OF WHAT WE NEED!

READ 'HOW TO DECRYPT' TXT-FILE
ON YOUR DESKTOP FOR DETAILS

JUST DO IT AS FAST AS YOU CAN!

REMEMBER: DON'T TRY TO TELL SOMEONE
ABOUT THIS MESSAGE IF YOU WANT TO GET
YOUR FILES BACK! JUST DO ALL WE TOLD.

Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

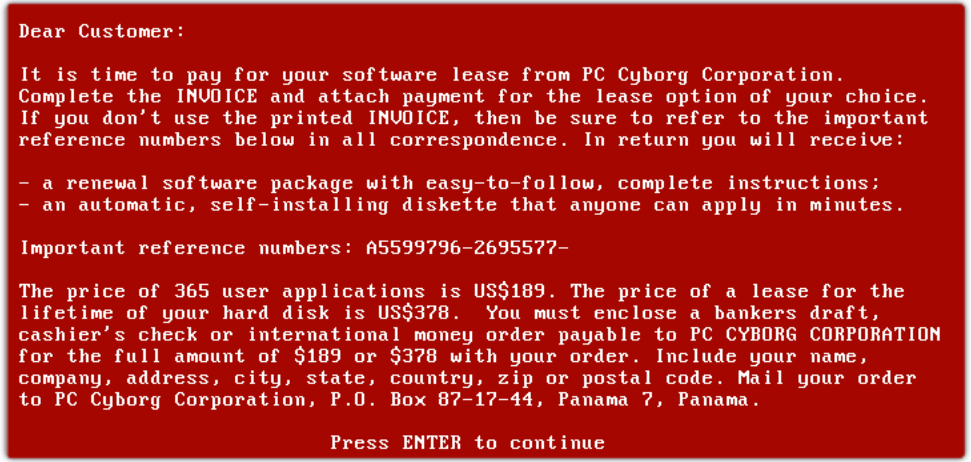
bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

The First Ransomware - 1989



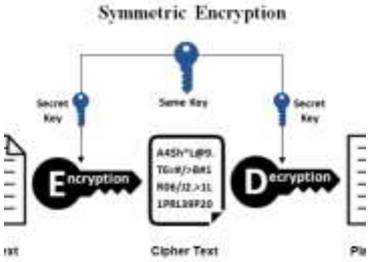
```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                          Press ENTER to continue
```

AIDS Information
Introductory Diskette Version 2.0
1. Boot your computer
2. Insert this diskette into drive A
3. At the C> prompt, type A:INSTALL
4. Press ENTER

The First Ransomware - The AIDS Trojan

Delivery

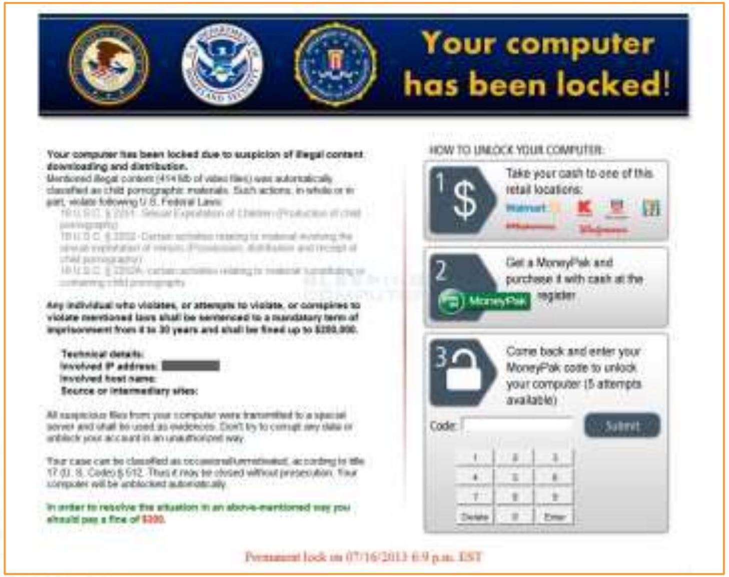
Encryption



Business Model

Encryption

Screen lockers (2010)



Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251 - Sexual Exploitation of Children (Production of child pornography)

18 U.S.C. § 2252 - Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A - certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [redacted]
Involved host name:
Source or intermediary sites:

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

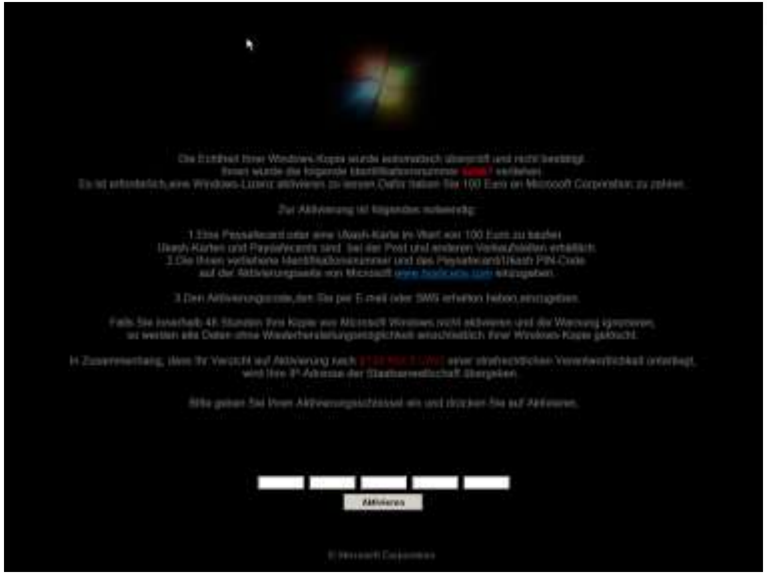
1 Take your cash to one of this retail locations:

2 Get a MoneyPak and purchase it with cash at the register

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code:

Permanent lock on 07/16/2013 6:9 p.m. EST



Die Echtheit Ihrer Windows-Kopie wurde automatisch überprüft und nicht bestätigt.
Ihnen wurde die folgende Identifikationsnummer [illegible] verliehen.
Es ist erforderlich,eine Windows-Lizenz aktivieren zu lassen.Dafür haben Sie 100 Euro an Microsoft Corporation zu zahlen.

Zur Aktivierung ist folgendes notwendig:

1.Eine Paysafecard oder eine Ukash-Karte im Wert von 100 Euro zu kaufen.
Ukash-Karten und Paysafecards sind bei der Post und anderen Verkaufsstellen erhältlich.
2.Die Ihnen verliehene Identifikationsnummer und den Paysafecard/Ukash PIN-Code
auf der Aktivierungsseite von Microsoft [illegible] eingegeben.

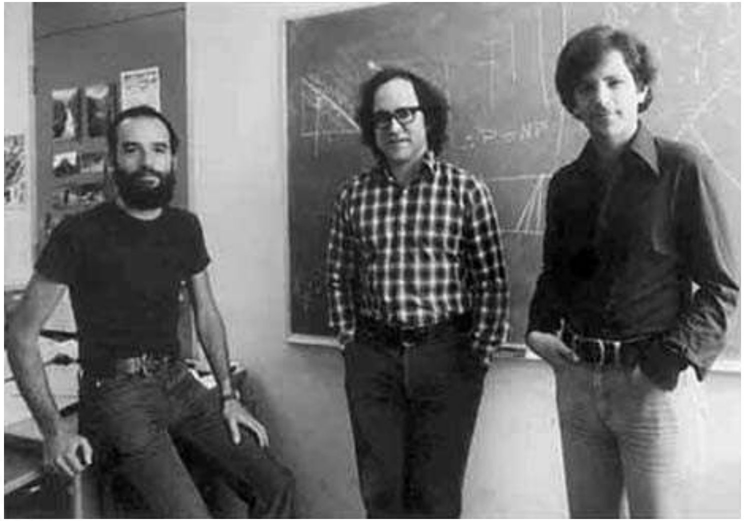
3.Den Aktivierungscode,den Sie per E-mail oder SMS erhalten haben,eingegeben.

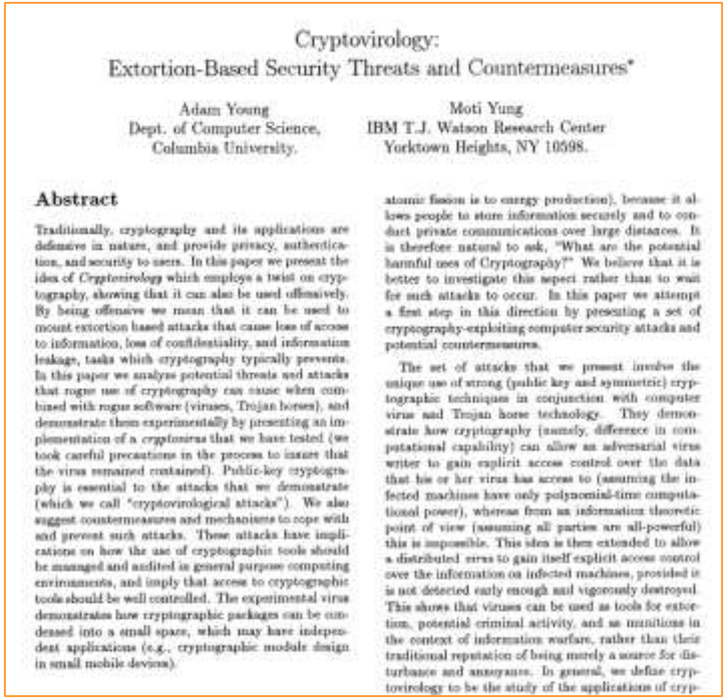
Falls Sie innerhalb 48 Stunden Ihre Kopie von Microsoft Windows nicht aktivieren und die Warnung ignorieren,
so werden alle Daten ohne Wiederherstellungsmöglichkeit einschließlich Ihrer Windows-Kopie gelöscht.

In Zusammenhang, dass Ihr Verzicht auf Aktivierung nach [illegible] einer strafrechtlichen Verantwortlichkeit unterliegt,
wird Ihre IP-Adresse der Staatsanwaltschaft übergeben.

Bitte geben Sie Ihren Aktivierungsschlüssel ein und drücken Sie auf Aktivieren.

Cryptoviral Extortion/Asymmetric Encryption (1996)





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.

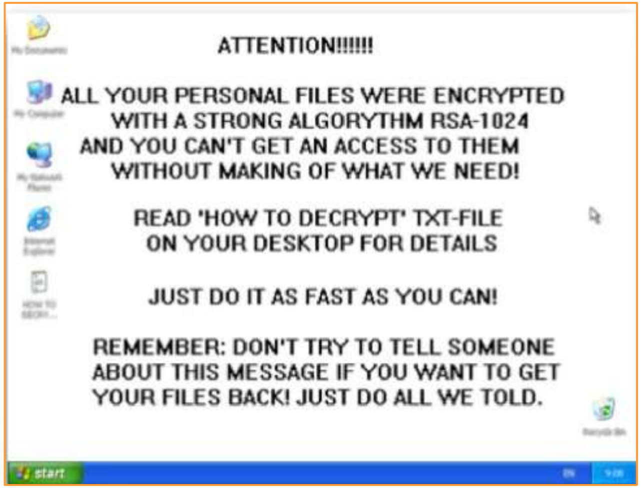
Abstract

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 leakage, tasks which cryptography typically prevents. In this paper we analyse potential threats and attacks that rogue use of cryptography can cause when combined with rogue software (viruses, Trojan horses), and demonstrate them experimentally by presenting an implementation of a *cryptovirus* that we have tested (we took careful precautions in the process to insure that the virus remained contained). Public-key cryptography is essential to the attacks that we demonstrate (which we call "cryptovirological attacks"). We also suggest countermeasures and mechanisms to cope with and prevent such attacks. These attacks have implications on how the use of cryptographic tools should be managed and audited in general purpose computing environments, and imply that access to cryptographic tools should be well controlled. The experimental virus demonstrates how cryptographic packages can be condensed into a small space, which may have independent applications (e.g., cryptographic module design in small mobile devices).

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 cryptography-exploiting computer security attacks and potential countermeasures.

The set of attacks that we present involve the unique use of strong (public key and symmetric) cryptographic techniques in conjunction with computer virus and Trojan horse technology. They demonstrate how cryptography (namely, difference in computational capability) can allow an adversarial virus writer to gain explicit access control over the data that his or her virus has access to (assuming the infected machines have only polynomial-time computational power), whereas from an information theoretic point of view (assuming all parties are all-powerful) this is impossible. This idea is then extended to allow a distributed virus to gain itself explicit access control over the information on infected machines, provided it is not detected early enough and vigorously destroyed. This shows that viruses can be used as tools for extortion, potential criminal activity, and as munitions in the context of information warfare, rather than their traditional reputation of being merely a source for disturbance and annoyance. In general, we define cryptovirology to be the study of the applications of cryp-

RSA Encrypted- GPCode (2006)



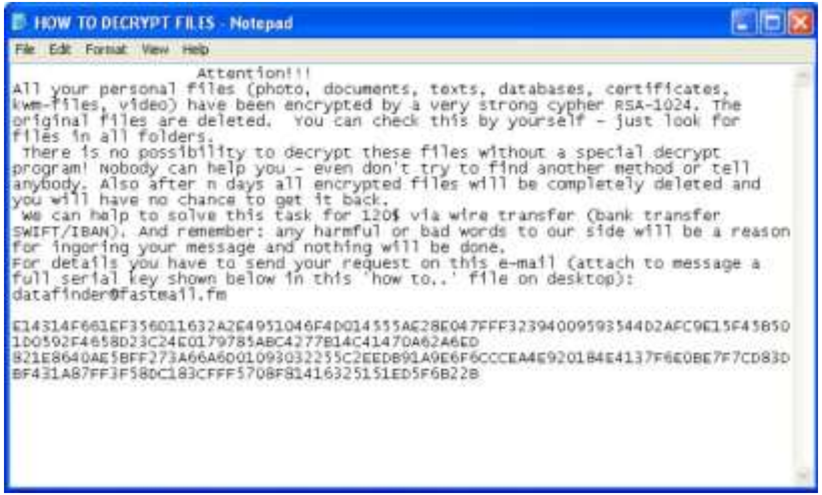
ATTENTION!!!!!!

ALL YOUR PERSONAL FILES WERE ENCRYPTED WITH A STRONG ALGORYTHM RSA-1024 AND YOU CAN'T GET AN ACCESS TO THEM WITHOUT MAKING OF WHAT WE NEED!

READ 'HOW TO DECRYPT' TXT-FILE ON YOUR DESKTOP FOR DETAILS

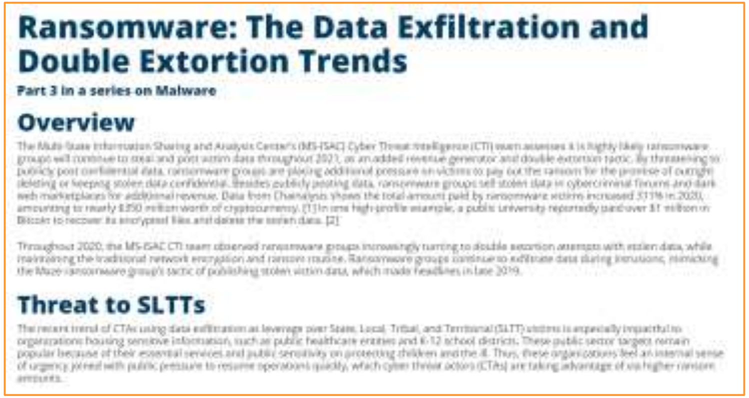
JUST DO IT AS FAST AS YOU CAN!

REMEMBER: DON'T TRY TO TELL SOMEONE ABOUT THIS MESSAGE IF YOU WANT TO GET YOUR FILES BACK! JUST DO ALL WE TOLD.



```
                  Attention!!!
All your personal files (photo, documents, texts, databases, certificates,
kwm-files, video) have been encrypted by a very strong cypher RSA-1024. The
original files are deleted.  You can check this by yourself - just look for
files in all folders.
 There is no possibility to decrypt these files without a special decrypt
program! Nobody can help you - even don't try to find another method or tell
anybody. Also after n days all encrypted files will be completely deleted and
you will have no chance to get it back.
 We can help to solve this task for 120$ via wire transfer (bank transfer
SWIFT/IBAN). And remember: any harmful or bad words to our side will be a reason
for ingoring your message and nothing will be done.
For details you have to send your request on this e-mail (attach to message a
full serial key shown below in this 'how to..' file on desktop):
datafinder@fastmail.fm

E14314F661EF356011632A2E4951046F4D014555AE28E047FFF32394009593544D2AFC9E15F45B50
1D0592F4658D23C24E0179785ABC4277B14C41470A62A6ED
B21E8640AE5BFF273A66A6D01093032255C2EEDB91A9E6F6CCCEA4E92018 4E4137F6E0BE7F7CD83D
BF431A87FF3F58DC183CFFF5708F81416325151ED5F6B22B
```

Exfiltrating Ransomware (Late 2010's)



Ransomware: The Data Exfiltration and Double Extortion Trends

Part 3 in a series on Malware

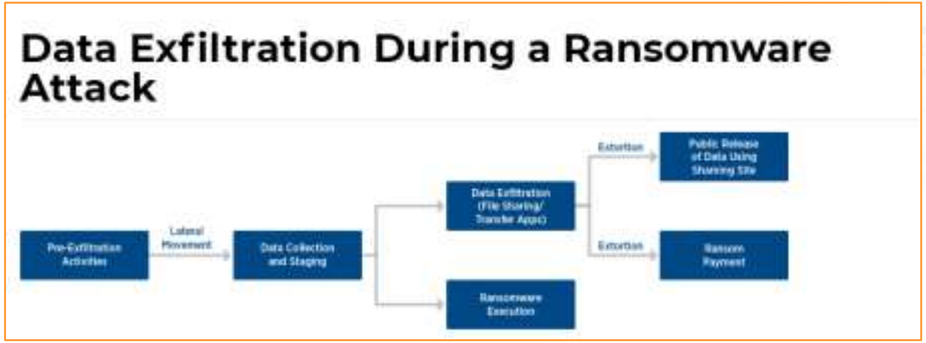
Overview

The Multi-State Information Sharing and Analysis Center's (MS-ISAC) Cyber Threat Intelligence (CTI) team assesses it is highly likely ransomware groups will continue to steal and post victim data throughout 2021, as an added revenue generator and double extortion tactic. By threatening to publicly post confidential data, ransomware groups are placing additional pressure on victims to pay out the ransom for the promise of outright deleting or keeping stolen data confidential. Besides publicly posting data, ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue. Data from Chainalysis shows the total amount paid by ransomware victims increased 311% in 2020, amounting to nearly $350 million worth of cryptocurrency. [1] In one high-profile example, a public university reportedly paid over $1 million in Bitcoin to recover its encrypted files and delete the stolen data. [2]

Throughout 2020, the MS-ISAC CTI team observed ransomware groups increasingly turning to double extortion attempts with stolen data, while maintaining the traditional network encryption and ransom routine. Ransomware groups continue to exfiltrate data during intrusions, mimicking the Maze ransomware group's tactic of publishing stolen victim data, which made headlines in late 2019.

Threat to SLTTs

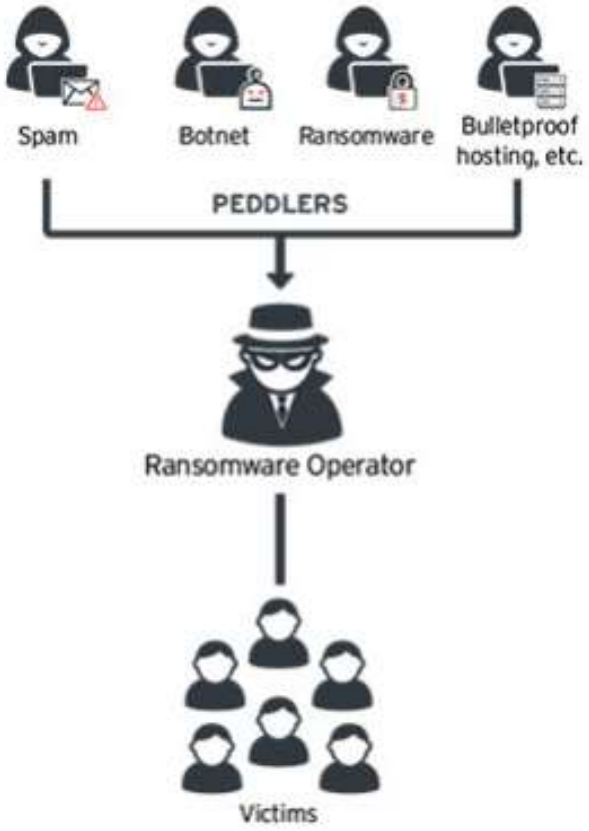
The recent trend of CTAs using data exfiltration as leverage over State, Local, Tribal, and Territorial (SLTT) victims is especially impactful to organizations housing sensitive information, such as public healthcare entities and K-12 school districts. These public sector targets remain popular because of their essential services and public sensitivity on protecting children and the ill. Thus, these organizations feel an internal sense of urgency joined with public pressure to resume operations quickly, which cyber threat actors (CTAs) are taking advantage of via higher ransom amounts.



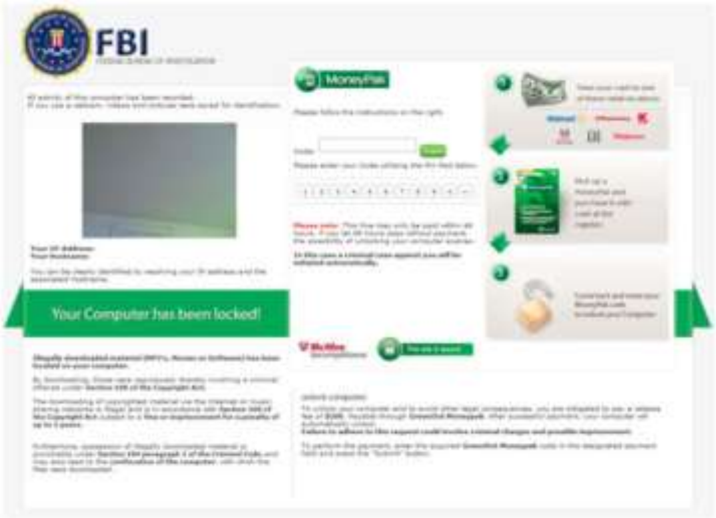
Data Exfiltration During a Ransomware Attack

Pre-Exfiltration Activities
Lateral Movement
Data Collection and Staging
Data Exfiltration (File Sharing/ Transfer Apps)
Ransomware Execution
Extortion
Public Release of Data Using Sharing Site
Extortion
Ransom Payment

Business Model



Gift Cards/Prepaid Debit

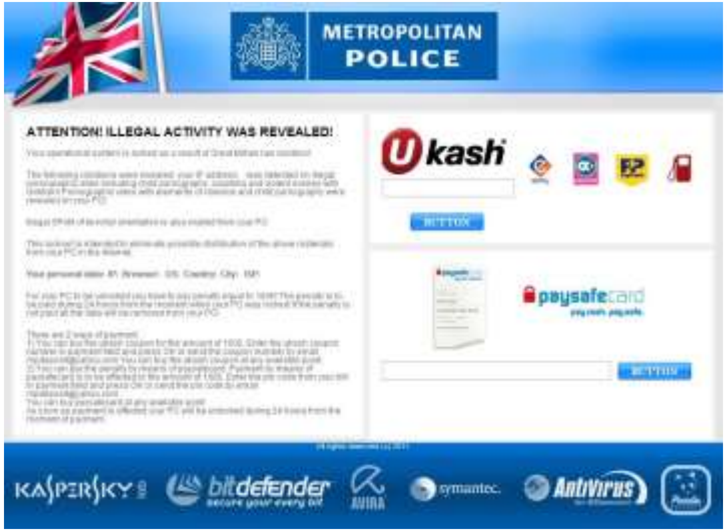


FBI

MoneyPak

Your Computer has been locked!

[illegible]

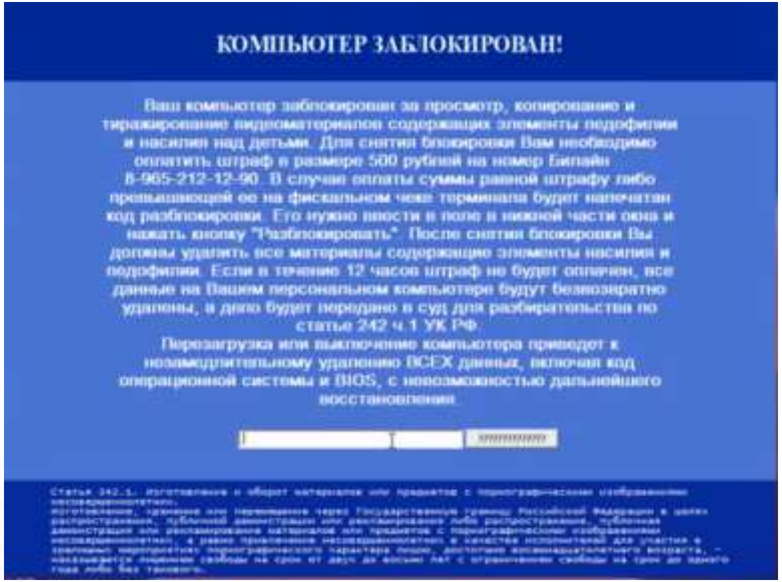


METROPOLITAN POLICE

ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!

[illegible]

Electronic Currencies



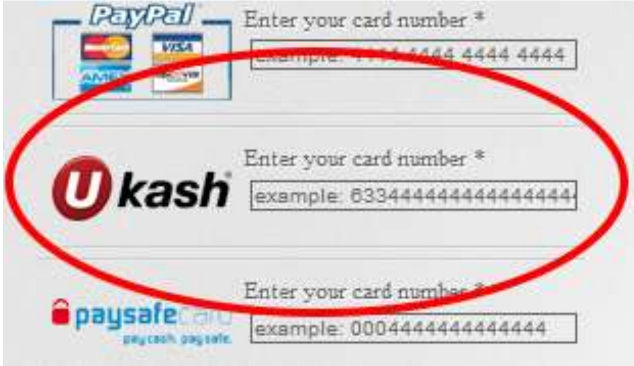
КОМПЬЮТЕР ЗАБЛОКИРОВАН!

Ваш компьютер заблокирован за просмотр, копирование и тиражирование видеоматериалов содержащих элементы педофилии и насилия над детьми. Для снятия блокировки Вам необходимо оплатить штраф в размере 500 рублей на номер Билайн 8-965-212-12-90. В случае оплаты суммы равной штрафу либо превышающей ее на фискальном чеке терминала будет напечатан код разблокировки. Его нужно ввести в поле в нижней части окна и нажать кнопку "Разблокировать". После снятия блокировки Вы должны удалить все материалы содержащие элементы насилия и педофилии. Если в течение 12 часов штраф не будет оплачен, все данные на Вашем персональном компьютере будут безвозвратно удалены, а дело будет передано в суд для разбирательства по статье 242 ч.1 УК РФ.

Перезагрузка или выключение компьютера приведет к незамедлительному удалению ВСЕХ данных, включая код операционной системы и BIOS, с невозможностью дальнейшего восстановления.

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних.

Изготовление, хранение или перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, а равно привлечение несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера лицом, достигшим восемнадцатилетнего возраста, - наказываются лишением свободы на срок от двух до восьми лет с ограничением свободы на срок до одного года либо без такового.



Enter your card number *

example: 4444 4444 4444 4444

Enter your card number *

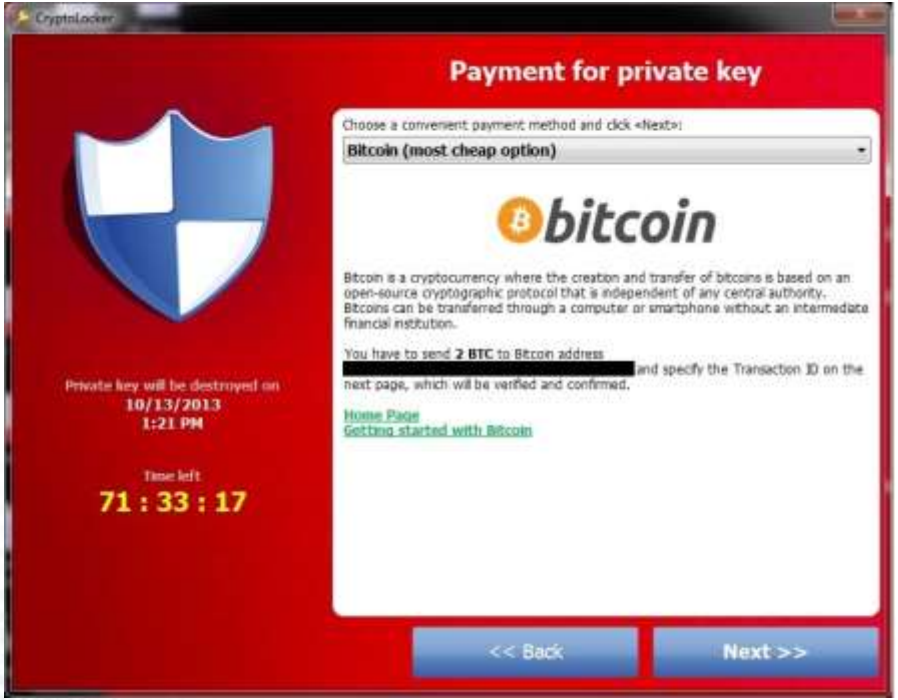
example: 633444444444444444

Enter your card number *

example: 0004444444444444

e-gold

Bitcoin (2013)



Payment for private key

Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 17

Choose a convenient payment method and click <Next>:

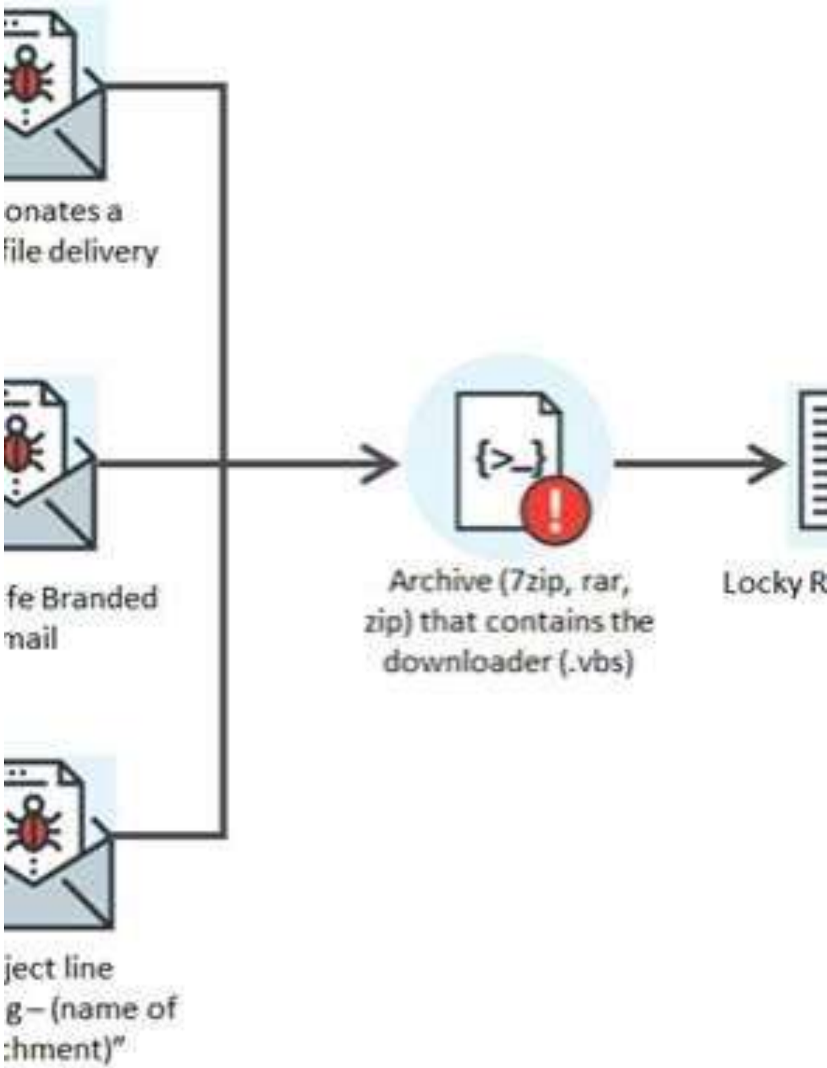
Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

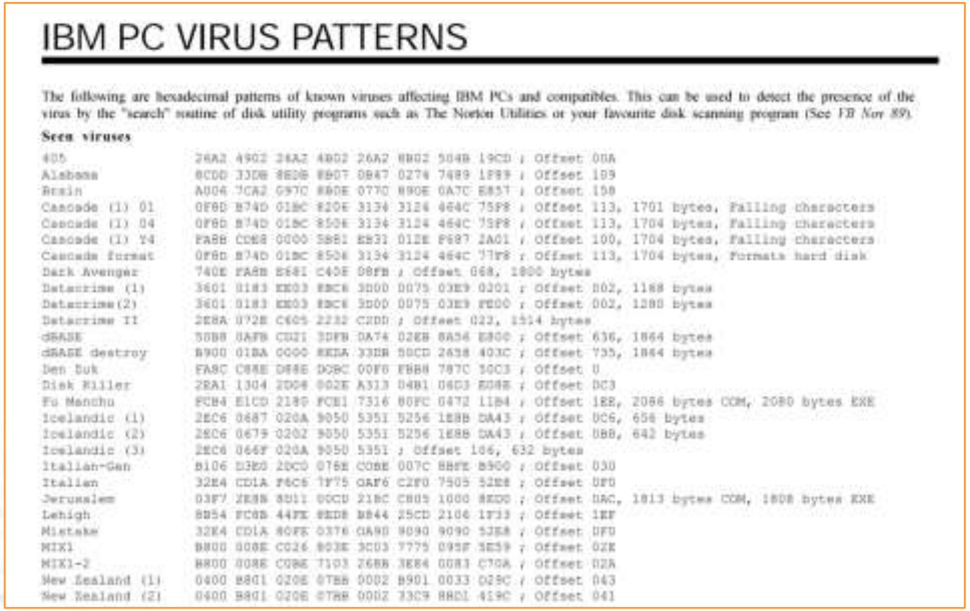
Home Page
Getting started with Bitcoin

Delivery


onates a
file delivery
fe Branded
mail
ject line
g – (name of
chment)”
{>_}
Archive (7zip, rar, zip) that contains the downloader (.vbs)
Locky R

The “Sneakernet”- 1980’s, 1990’s

(Technically includes modern USB)

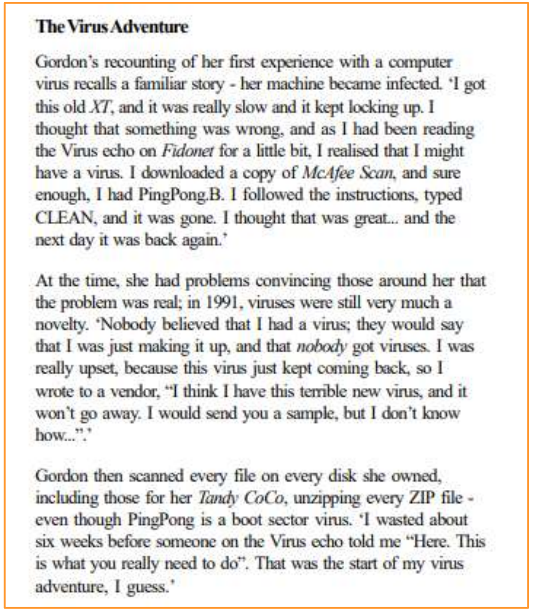


IBM PC VIRUS PATTERNS

The following are hexadecimal patterns of known viruses affecting IBM PCs and compatibles. This can be used to detect the presence of the virus by the "search" routine of disk utility programs such as The Norton Utilities or your favourite disk scanning program (See *FB Nov 89*).

Seen viruses

```
405                 26A2 4902 26A2 4B02 26A2 8B02 504B 19CD ; Offset 00A
Alabama             8CDD 33DB 8EDB 8B07 0B47 0274 7489 1F89 ; Offset 109
Brain               A006 7CA2 097C 8B0E 077C 890E 0A7C E837 ; Offset 158
Cascade (1) 01      0F8D B74D 01BC 820E 3134 3124 464C 75F8 ; Offset 113, 1701 bytes, Falling characters
Cascade (1) 04      0F8D B74D 01BC 8506 3134 3124 464C 75F8 ; Offset 113, 1704 bytes, Falling characters
Cascade (1) Y4      FA8B CDE8 0000 5B81 EB31 012E F687 2A01 ; Offset 100, 1704 bytes, Falling characters
Cascade format      0F8D B74D 01BC 8506 3134 3124 464C 77F8 ; Offset 113, 1704 bytes, Formats hard disk
Dark Avenger        740E FA8B E681 C40E 08FB ; Offset 068, 1800 bytes
Datacrime (1)       3601 0183 EE03 8BCE 3D00 0075 03E9 0201 ; Offset 002, 1168 bytes
Datacrime(2)        3601 0183 EE03 8BCE 3D00 0075 03E9 FE00 ; Offset 002, 1280 bytes
Datacrime II        2E8A 072E C605 2232 C2DD ; Offset 022, 1514 bytes
dBASE               50B8 0AFB CD21 3DFB 0A74 02EB 8A56 E800 ; Offset 636, 1864 bytes
dBASE destroy       B900 01BA 0000 8EDA 33DB 50CD 2638 403C ; Offset 735, 1864 bytes
Den Zuk             FA8C C88E D88E D0BC 00F0 FBB8 787C 50C3 ; Offset 0
Disk Killer         2EA1 1304 2D08 002E A313 04B1 06D3 E08E ; Offset DC3
Fu Manchu           FCB4 E1CD 2180 FCE1 7316 80FC 0472 11B4 ; Offset 1EE, 2086 bytes COM, 2080 bytes EXE
Icelandic (1)       2EC6 0687 020A 9050 5351 5256 1E8B DA43 ; Offset 0C6, 656 bytes
Icelandic (2)       2EC6 0679 0202 9050 5351 5256 1E8B DA43 ; Offset 0B8, 642 bytes
Icelandic (3)       2EC6 066F 020A 9050 5351 ; Offset 106, 632 bytes
Italian-Gen         B106 D3E0 2DC0 076E C08E 007C 8BFE B900 ; Offset 030
Italian             32E4 CD1A F6C6 7F75 0AF6 C2F0 7505 52E8 ; Offset 0F0
Jerusalem           03F7 2E8B 8D11 00CD 21BC C805 1000 8ED0 ; Offset DAC, 1813 bytes COM, 1808 bytes EXE
Lehigh              8B54 FC8B 44FE 8ED8 B844 25CD 2106 1F33 ; Offset 1EF
Mistake             32E4 CD1A 80FE 0376 0A80 9090 9090 52E8 ; Offset 0F0
MIX1                B800 008E C026 803E 3C03 7775 095F 5E59 ; Offset 02E
MIX1-2              B800 008E C08E 7103 268B 3E84 0083 C70A ; Offset 02A
New Zealand (1)     0400 B801 020E 07BB 0002 B901 0033 D29C ; Offset 043
New Zealand (2)     0400 B801 020E 07BB 0002 33C9 8BD1 419C ; Offset 041
```



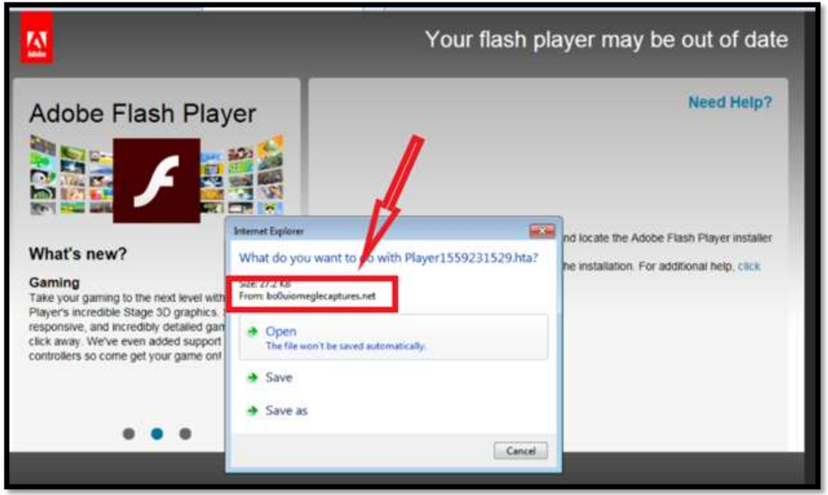
The Virus Adventure

Gordon’s recounting of her first experience with a computer virus recalls a familiar story - her machine became infected. ‘I got this old *XT*, and it was really slow and it kept locking up. I thought that something was wrong, and as I had been reading the Virus echo on *Fidonet* for a little bit, I realised that I might have a virus. I downloaded a copy of *McAfee Scan*, and sure enough, I had PingPong.B. I followed the instructions, typed CLEAN, and it was gone. I thought that was great... and the next day it was back again.’

At the time, she had problems convincing those around her that the problem was real; in 1991, viruses were still very much a novelty. ‘Nobody believed that I had a virus; they would say that I was just making it up, and that *nobody* got viruses. I was really upset, because this virus just kept coming back, so I wrote to a vendor, “I think I have this terrible new virus, and it won’t go away. I would send you a sample, but I don’t know how...”.’

Gordon then scanned every file on every disk she owned, including those for her *Tandy CoCo*, unzipping every ZIP file - even though PingPong is a boot sector virus. ‘I wasted about six weeks before someone on the Virus echo told me “Here. This is what you really need to do”. That was the start of my virus adventure, I guess.’

“Spam” Email and Exploit kits - late 90’s until today



Your flash player may be out of date

Adobe Flash Player

What's new?

Gaming

Take your gaming to the next level with Player's incredible Stage 3D graphics. responsive, and incredibly detailed gam click away. We've even added support controllers so come get your game on!

Need Help?

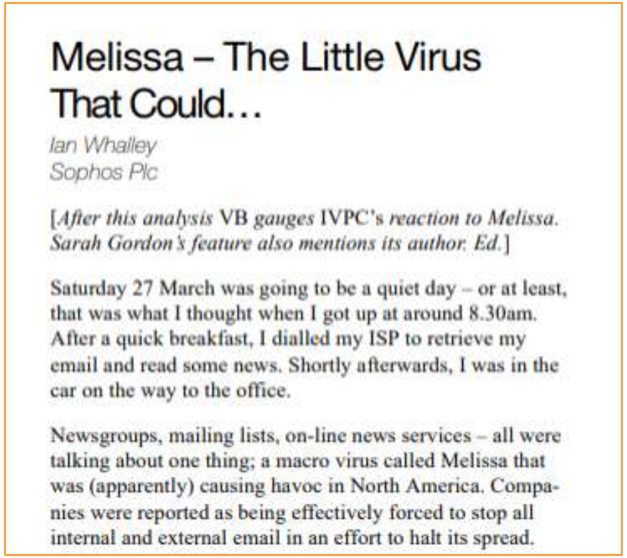
nd locate the Adobe Flash Player installer he installation. For additional help, click

Internet Explorer

What do you want to do with Player1559231529.hta?

Size: 27.2 KB
From: bo0uiomeglecaptures.net

Open
The file won't be saved automatically.
Save
Save as
Cancel



Melissa – The Little Virus That Could…

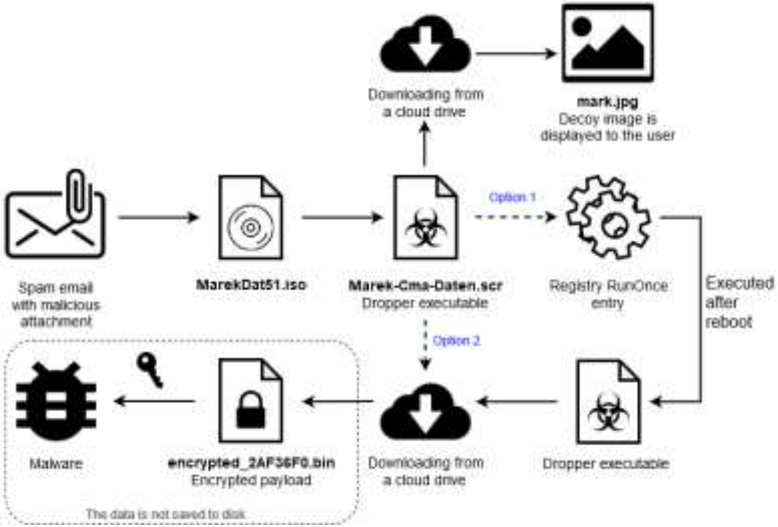
Ian Whalley
Sophos Plc

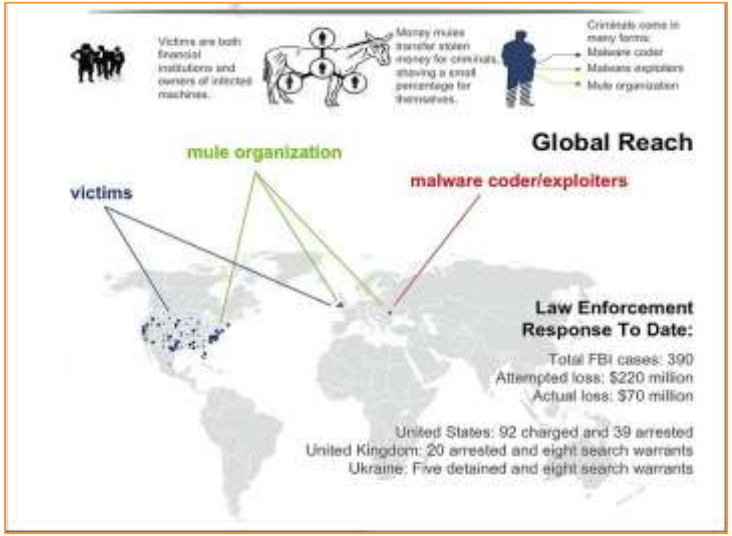
[*After this analysis* VB *gauges* IVPC*’s reaction to Melissa. Sarah Gordon’s feature also mentions its author. Ed.*]

Saturday 27 March was going to be a quiet day – or at least, that was what I thought when I got up at around 8.30am. After a quick breakfast, I dialled my ISP to retrieve my email and read some news. Shortly afterwards, I was in the car on the way to the office.

Newsgroups, mailing lists, on-line news services – all were talking about one thing; a macro virus called Melissa that was (apparently) causing havoc in North America. Companies were reported as being effectively forced to stop all internal and external email in an effort to halt its spread.

Trojans, Botnets, Multistage Attacks, and Malware as a Service (2010)





Victims are both financial institutions and owners of infected machines.

Money mules transfer stolen money for criminals, shaving a small percentage for themselves.

Criminals come in many forms:
- Malware coder
- Malware exploiters
- Mule organization

Global Reach

mule organization

victims

malware coder/exploiters

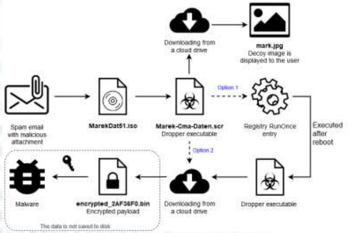
Law Enforcement Response To Date:

Total FBI cases: 390
Attempted loss: $220 million
Actual loss: $70 million

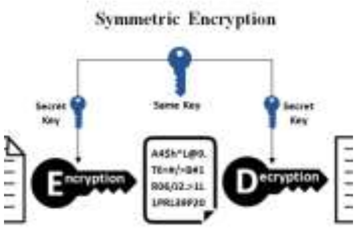
United States: 92 charged and 39 arrested
United Kingdom: 20 arrested and eight search warrants
Ukraine: Five detained and eight search warrants

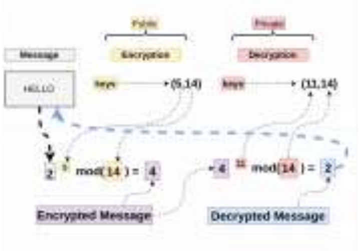
The Evolution of Ransomware

Delivery

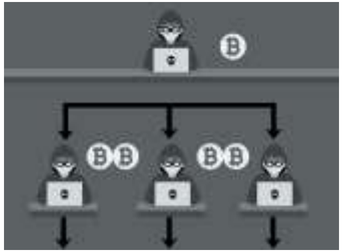


Encryption





Business Model



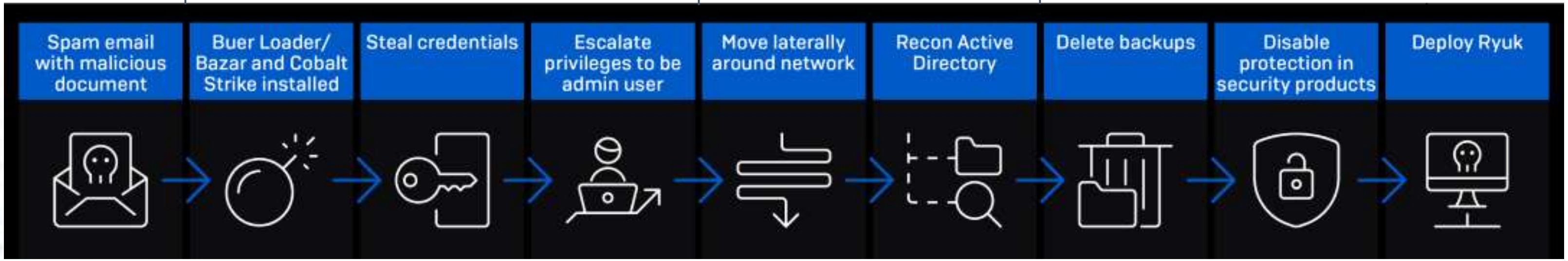
Disrupting the Attackers

Pre-Infection

During Infection

Recon & Lateral Movement

Detonation



Spam email with malicious document → Buer Loader/ Bazar and Cobalt Strike installed → Steal credentials → Escalate privileges to be admin user → Move laterally around network → Recon Active Directory → Delete backups → Disable protection in security products → Deploy Ryuk