第十五届CCFC计算机取证技术峰会暨展会

THE 15TH CHINA COMPUTER FORENSIC CONFERENCE & EXHIBITION

电子数据取证技术最新发展与应用

2019.11.5 -11.7

武汉市·荷田大酒店

以AI技术对恶意代码取证分析

ABOUT ME

•张志宋 博士

- 华梵大学机电工程学院(计算机组)博士
- 研究领域:
  - 网络安全、信息安全政策、网络攻防、数字取证、高科技犯罪、科技法律、信息伦理与个人讯息保护
- 国际证照: ii
  - BS 7799/ISO 27001 LA (ISMS)信息安全管理系统
  - BS 15000/ISO 20000 LA (ITSM)信息科技服务管理
  - BS 25999/ISO 22301 LA (BCM) 持续营运管理
  - CHFI(Computer Hacking Forensic Investigator)信息安全取证专家调查
  - CEH(Certified Ethical Hacker)道德黑客技术专家
  - BS 10012/ISO 29100 LA (PIMS)个人讯息保护管理
  - ISO27005信息风险管理

CONTENTS

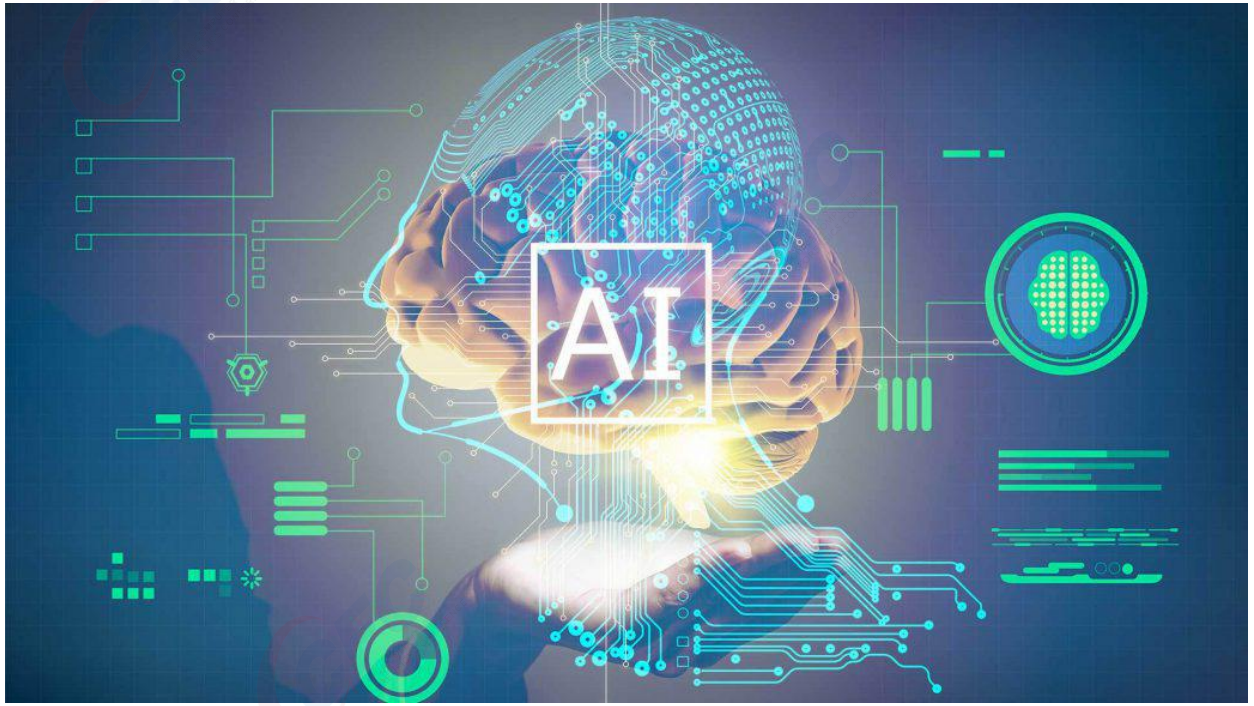
1 主动学习（Active learning）

2 特征萃取

3 案例

PART ONE

主动学习
（Active learning）



主动学习（Active learning）

- 主动学习是一种使机器能够学习的机器学习设置巧妙地“问问题”以减少标签工作。
- 主动学习的工作侧重于改变将问题的提问，变为可编程的原理策略。
- 当原理策略恰好与现有数据集的特征相匹配，相应的策略可以带来实践性能。但并非所有原理策略都可满足每个特点数据集。（例如逻辑关系）

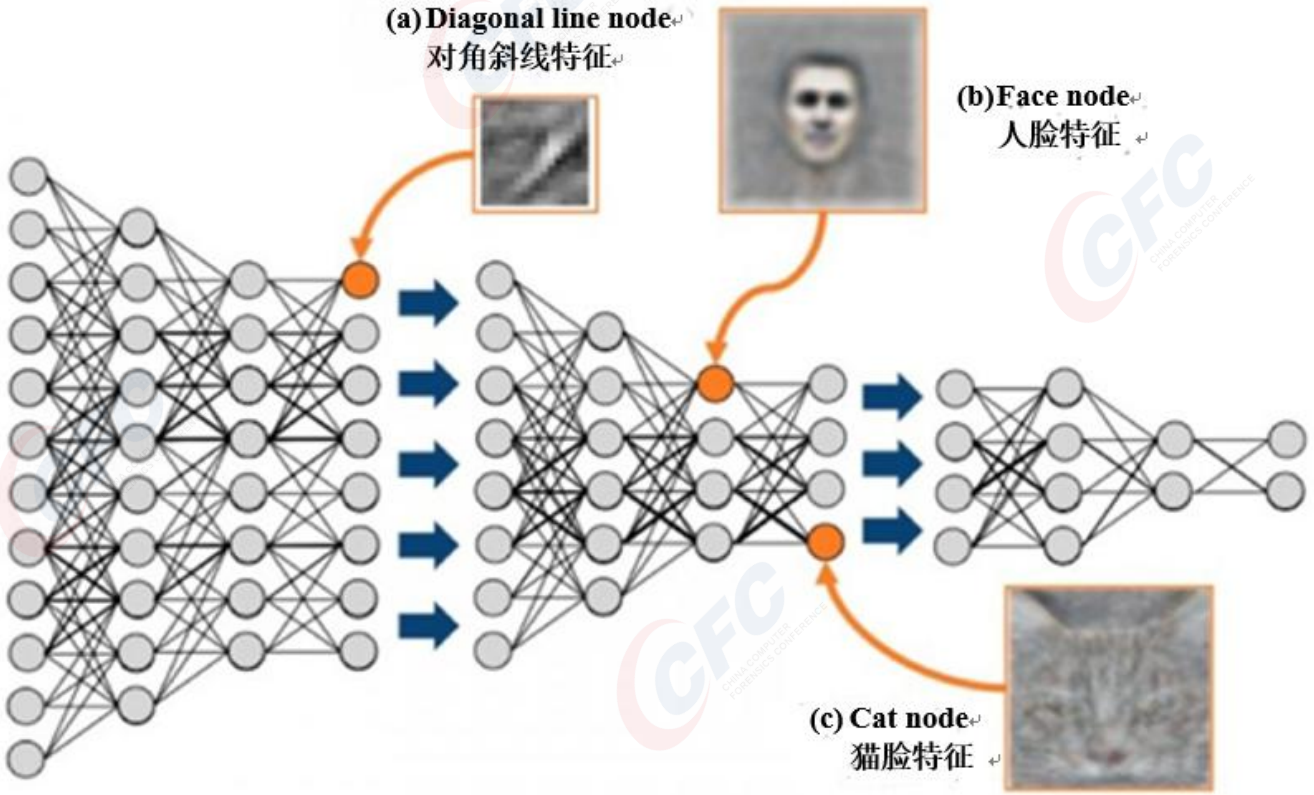
主动学习（Active learning）

- 虽然主动学习，可以通过学习训练，完成非常强悍的人工智能功能，但是目前为止，主动学习还无法理解所谓的”逻辑关系”，好像主动学习可以识别出女人、老人、小孩，但无法识别出爸爸、儿子、祖父、异卵双胞胎这些概念，更不可能理解这些不同男性之间的关系，原因在于主动学习的学习训练样本并不包括相关概念。

- 在这一点上，区块链或许就有用武之地，因为区块链是过程数据的管理技术，所有记录在链的数据都具有先后逻辑顺序，如果有目的地将区块链上数据设定为具有逻辑顺序的训练样本，那么深度学习就可以通过对区块链上数据的学习，将数据的快照讯息与数据的过程讯息结合在一起，从而”学会”更加抽象的概念。

主动学习（Active learning）

- 主动学习的原理，它仍然是模拟神经网络的构成，有一个输入层和一个输出层，在这两个神经元层之间，可以设置无限多个隐藏层，每一个隐藏层上都有很多感知器（类似神经元），每一个感知器都有一个阈值，阈值的作用就像”阀门”，当感知器的输入低于阈值时、则该感知器向下层输出”0”，反之，当感知器的输入高于阈值时、则感知器向下层输出”1”。
- 不同的输入，经过多个隐藏层多个感知器不同组合的传递，就可以最终输出不同结果，或者说针对不同感知、做出不同反应。



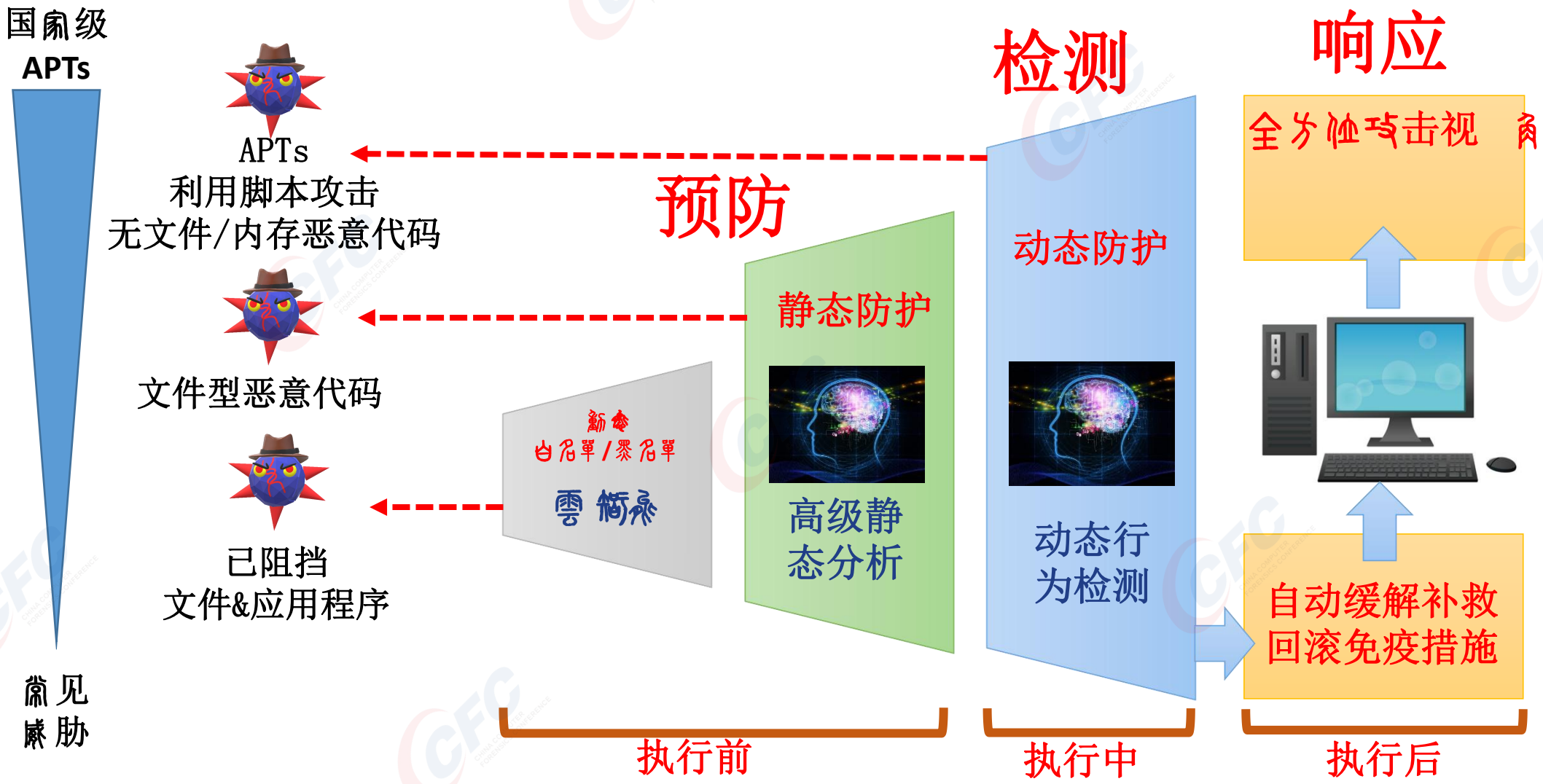
主动学习（Active learning）

- 主动学习可以分为两类：
  - 基于数据流（ stream-based）在基于流的主动学习中，每个实例是从数据流中的某些分布中提取的方式，学习者必须立即决定是否查询该实例的标签与否。 虽然他们的数据访问受到更多限制，基于流的主动学习算法一般都会来具有更可靠的理论性能保证。
  - 基于数据池（ pool-based）的主动学习更加现实的设置，可以更灵活地访问数据并将成为本文的重点。基于池主动学习问题，向学习者介绍开始时是未标记的池和标记的池。代表性抽样解决了不确定性的警告兼顾不确定性和代表性实例的数量。研究人员提出各种测量的代表性。

主动学习（Active learning）

- 黑客的攻击手法不断创新，已经无法完全依靠传统的专家规则进行侦测防范。
- 倘若可以透过人机协作的方式，网络安全取证专家便能订定各种恶意威胁的特征与学习策略，以此作为训练模型的基础，并藉由模型自主提问与专家反馈的方式来成长茁壮。
- 当训练趋近成熟时，模型便可视为一位网络安全取证，辅助企业解决络安全问题，将节省的人事资源投入至其他所需之处。
- 例：网络连线的定义为在某段时间内，从开始到结束的TCP数据包序列，且在这段时间内数据在协议（例：TCP、UDP）下从来源IP至目的IP的传递。每个网络连接皆会被标记正常或异常，区分异常类型、未知攻击、训练资料等各种攻击手法。

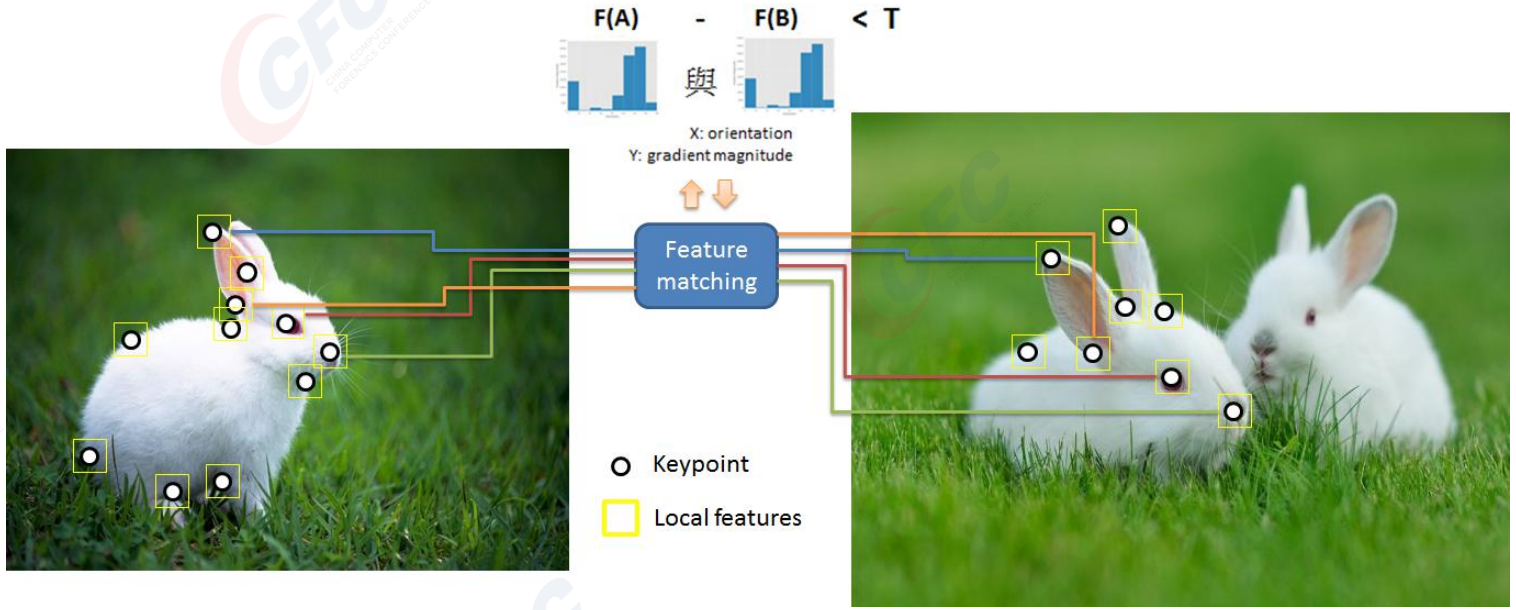
事前预防 事中侦测、事后响应



以非监督式的主动学习技术，实作事前预防、事中侦测、事后响应，以及整体恶意代码的调查取证数据

PART TWO

特征萃取



特征萃取

- 原始数据为恶意代码的asm与bytes文件，其分别为相关的后设文件（Metadata）与16进制表示（Hexadecimal Representation）的二位元（Binary）文件。
- 后设数据，含有字串（Strings）、函式呼叫（Function Calls）等重要数据。
- 恶意代码式家族的特性会反映在bytes和asm文件中，所以为了能够有效地进行分类，必需透过特征萃取产生具识别意义的特征。

特征萃取

```
.text:00401000 ;
.text:00401000 ; +-------------------------------------------------------------------------+
.text:00401000 ; |   This file has been generated by The Interactive Disassembler (IDA)    |
.text:00401000 ; |           Copyright (c) 2017 Hex-Rays, <support@hex-rays.com>           |
.text:00401000 ; |                         License info: 48-3FBD-7F04-2C                   |
.text:00401000 ; |                         Jiang Ying, Personal license                    |
.text:00401000 ; +-------------------------------------------------------------------------+
.text:00401000 ;
.text:00401000 ; Input SHA256 : A70EDA16FC38789877FA3E74692818FB0CD87ED0DA683202D616C2E6C5A4104C
.text:00401000 ; Input MD5    : DC544F1F4BECC4A9DDB18FB09317ED68
.text:00401000 ; Input CRC32  : C088953B
.text:00401000
.text:00401000 ; File Name   : C:\virus\MinerGate-8.3-win64.exe
.text:00401000 ; Format      : Portable executable for 80386 (PE)
.text:00401000 ; Imagebase   : 400000
.text:00401000 ; Timestamp   : 597FCC6D (Tue Aug 01 00:33:49 2017)
.text:00401000 ; Section 1. (virtual address 00001000)
.text:00401000 ; Virtual size                  : 00005ED2 (  24274.)
.text:00401000 ; Section size in file          : 00006000 (  24576.)
.text:00401000 ; Offset to raw data for section: 00000400
.text:00401000 ; Flags 60000020: Text Executable Readable
.text:00401000 ; Alignment     : default
.text:00401000
.text:00401000                 .686p
.text:00401000                 .mmx
.text:00401000                 .model flat
.text:00401000
.text:00401000 ; ===========================================================================
.text:00401000
.text:00401000 ; Segment type: Pure code
.text:00401000 ; Segment permissions: Read/Execute
00000400 0000000000401000: sub_401000 (Synchronized with Hex View-1)
```

后设数据（Metadata）的asm文件

特征萃取

```
00401000  55 8B EC 83 EC 5C 83 7D  0C 0F 74 2B 83 7D 0C 46  U  ·㊫·\T··t+T··F
00401010  8B 45 14 75 0D 83 48 18  10 8B 0D 08 37 42 00 89    ··u.  ·····7B··
00401020  48 04 50 FF 75 10 FF 75  0C FF 75 08 FF 15 04 72  H.P.u..u..u....r
00401030  40 00 E9 42 01 00 00 53  56 8B 35 14 37 42 00 8D  @.囑···SV...7B..
00401040  45 A4 57 50 FF 75 08 FF  15 08 72 40 00 83 65 F4  E上·P.u....r@.  ··
00401050  00 89 45 0C 8D 45 E4 50  FF 75 08 FF 15 0C 72 40  .  ··  ·谽·.u....r@
00401060  00 8B 7D F0 83 65 F0 00  8B 1D 5C 70 40 00 E9 80  .  ··.e....\p@...
00401070  00 00 00 0F B6 46 52 0F  B6 56 56 0F AF 55 E8 8B  ....訶·R.越·V.狹··.
00401080  CF 2B 4D E8 0F AF C1 03  C2 89 4D 10 99 F7 FF 33  ..M..索·...M.  ··3
00401090  D2 8A F0 0F B6 46 51 0F  AF C1 0F B6 4E 55 0F AF  ....訶·Q.索··賁·U..
004010A0  4D E8 03 C1 8B CA 99 F7  FF 0F B6 56 54 0F AF 55  M.........越·T.狹·
004010B0  E8 8A C8 0F B6 46 50 0F  AF 45 10 03 C2 99 F7 FF  ....訶·P.浩·......
004010C0  C1 E1 08 0F B6 C0 0B C8  8D 45 F4 50 89 4D F8 FF  鏡··黃···E曨·  ···
004010D0  15 64 70 40 00 83 45 F0  04 89 45 14 50 8D 45 E4  .dp@.  ···  ··P  ··
004010E0  50 FF 75 0C FF 15 10 72  40 00 FF 75 14 FF D3 83  P.u....r@..u....
004010F0  45 E8 04 39 7D E8 0F 8C  77 FF FF FF 83 7E 58 FF  E..9}..  ···í·X.
00401100  74 65 FF 76 34 FF 15 54  70 40 00 85 C0 89 45 14  te.v4..Tp@.  ·  ··
00401110  74 55 8B 7D 0C 6A 01 57  C7 45 E4 10 00 00 00 C7  tU  ··j.W·......
00401120  45 E8 08 00 00 00 FF 15  50 70 40 00 FF 76 58 57  E.......Pp@..vXW
00401130  FF 15 58 70 40 00 FF 75  14 8B 35 4C 70 40 00 57  ..Xp@..u...Lp@.W
00401140  FF D6 89 45 0C 8D 45 E4  68 20 08 00 00 50 6A FF  ...E.  ·郭··...Pj.
00401150  68 00 2F 42 00 57 FF 15  14 72 40 00 FF 75 0C 57  h./B.W...r@..u.W
00401160  FF D6 FF 75 14 FF D3 8D  45 A4 50 FF 75 08 FF 15  ...u....E匕·.u...
00401170  6C 72 40 00 5F 5E 33 C0  5B C9 C2 10 00 8B 4C 24  lr@. ^3頤·匟·..  ·$
00401180  04 A1 48 37 42 00 8B D1  53 69 D2 18 04 00 00 56  .?·7B.  ·Si.....V
00401190  57 8B 54 02 08 F6 C2 02  74 4F 8D 71 01 33 FF 3B  W  ··.鷈·.tO  ··3.;
004011A0  35 4C 37 42 00 73 42 8B  CE 69 C9 18 04 00 00 8D  5L7B.sB  ·i......
004011B0  44 01 08 8B 08 F6 C1 02  74 03 47 EB 1E F6 C1 04  D....鶄·.t.G..鶄·.
004011C0  74 09 8B CF 4F 85 C9 74  20 EB 10 F6 C1 10 75 0B  t.  ·O  ·t··.鶄·.u.
004011D0  8B D9 33 DA 83 E3 01 33  D9 89 18 46 05 18 04 00    ·3....3...F....
004011E0  00 3B 35 4C 37 42 00 72  CA 5F 5E 5B C2 04 00 55  .;5L7B.r佤·^[...U
```

16进制表示（Hexadecimal Representation）的二位元（Binary） bytes文件

统计量

- 依据恶意代码家族的特性，其代码内容的常用指令也会有所不同，故针对asm 与bytes文件统计各指令之个数，并作为后续分析之特征使用。
- 其中，部分指令可能仅出现在少数特定代码中，抑或较无鉴别能力。
- 为了避免特征矩阵过于稀疏（Sparse）或无用，订定合适的筛选条件（例：各个恶意代码家族中最常出现的前500名）与指令清单，以此强化特征之功效。

统计量

- 下列为适合统计个数或比例之讯息：
  - 单一位元组频率（Single Byte Frequency）
  - 指令个数 / 比例（Instruction Count/Proportion）
  - 符号个数（Symbol Count）

    特殊符号（例：-、+、*、]、[、?、@）可以用来躲避特定类型的侦测方式，所以当其出现次数越高时，表示越有可能属于恶意代码。

统计量

- API频率（API Frequency）

  部分恶意代码在执行时，会透过系统的API进行存取等动作。藉此特性，可以使用过往恶意代码常用的API来辨识所属家族类型。有些恶意代码仅使用Load Library API，达到动态载入其他所需API之目的，以此规避防毒软件的侦测。

- 暂存器的使用频率（The Frequency of Use of the Registers）

  暂存器的使用与目的有相当大的关系，虽然可藉由重新命名改变暂存器的名称，但在一定程度上仍可帮助辨识恶意代码家族的类型。

统计量

预定义区块个数 / 比例（Predefined Sections Count/Proportion）

PE的组成中包含一些预定义的区块，其个数或比例皆与恶意程式家族的特性有所关联。如下表所示，预定义区块的清单中包含 .text、.data、.bss、.rdata、.edata、.idata、.rsrc、.tls 和 .reloc 等。

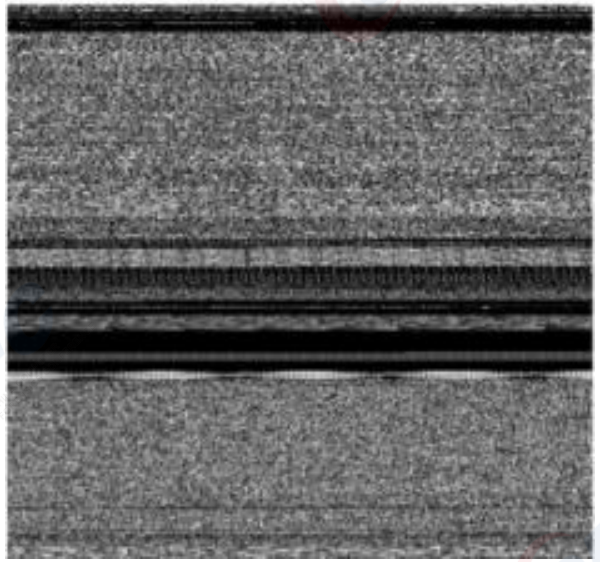
Name	Description
section_names_.bss	The total number of lines in .bss section
section_names_.data	The total number of lines in .data section
section_names_.edata	The total number of lines in .edata section
section_names_.idata	The total number of lines in .idata section
section_names_.rdata	The total number of lines in .rdata section
section_names_.rsrc	The total number of lines in .rsrc section
section_names_.text	The total number of lines in .text section
section_names_.tls	The total number of lines in .tls section
section_names_.reloc	The total number of lines in .reloc section
Num_Sections	The total number of sections
Unknown_Sections	The total number of unknown sections
Unknown_Sections_lines	The total number of lines in unknown sections
known_Sections_por	The proportion of known sections to the all section
Unknown_Sections_por	The proportion of unknown sections to the all sections
Unknown_Sections_lines_por	The proportion of the amount of unknown sections to the whole file
.text_por	The proportion of .text section to the whole file
.data_por	The proportion of .data section to the whole file
.bss_por	The proportion of .bss section to the whole file
.rdata_por	The proportion of .rdata section to the whole file
.edata_por	The proportion of .edata section to the whole file
.idata_por	The proportion of .idata section to the whole file
.rsrc_por	The proportion of .rsrc section to the whole file
.tls_por	The proportion of .tls section to the whole file
.reloc_por	The proportion of .reloc section to the whole file

统计量

- 除了一般常见的个数与比例等统计量之外，文件大小和字串长度等讯息也可以当作恶意代码家族分类的依据。
- 代码的指令乱度也能作为一特征，像是熵（Entropy）便可用来评估代码的随机性。当熵值越大时，表示其指令分布越无规律可言，即藏有恶意指令的可能性越低。且若任意两恶意代码的熵（Entropy）越接近，表示其程序指令的组成越相似，即越有可能来自同一恶意代码家族。

数据视觉化

由于asm与bytes文件中是以16进制表示的二位元组成，故转换为10进位制后的值域便落在0（黑）至255（白）之间，可直接以灰阶图方式呈现文件内容。为 asm 与bytes的灰阶图，可以发现后者的结果较前者来的明显有效，且依据不同恶意代码家族的特性，图也可能会有不同的样态。

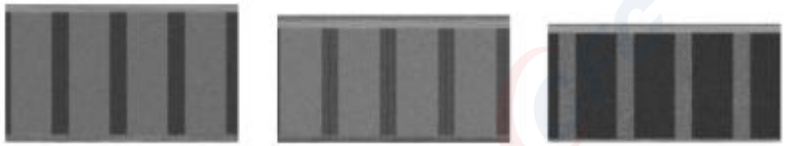


恶意代码的bytes图（左）& asm图（右）

Ref.: Microsoft Malware Classification Challenge (Big 2015): First Place Team: Say No to Overfitting

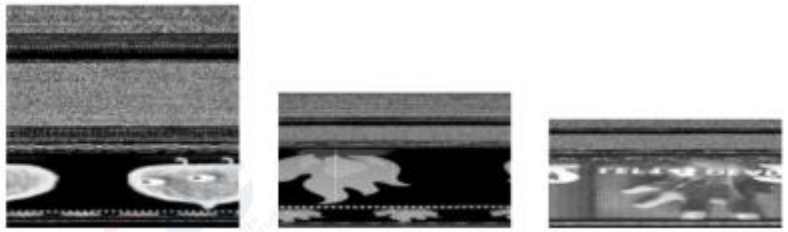
数据视觉化

1.三个恶意软件样本



2.三个恶意软件样本

3.三个不同几乎相似的图像



4.嵌入恶意代碼图像

恶意代码样本的图像

Ref.: Novel Feature Extraction, Selection and Fusion for Effective Malware Family Classification

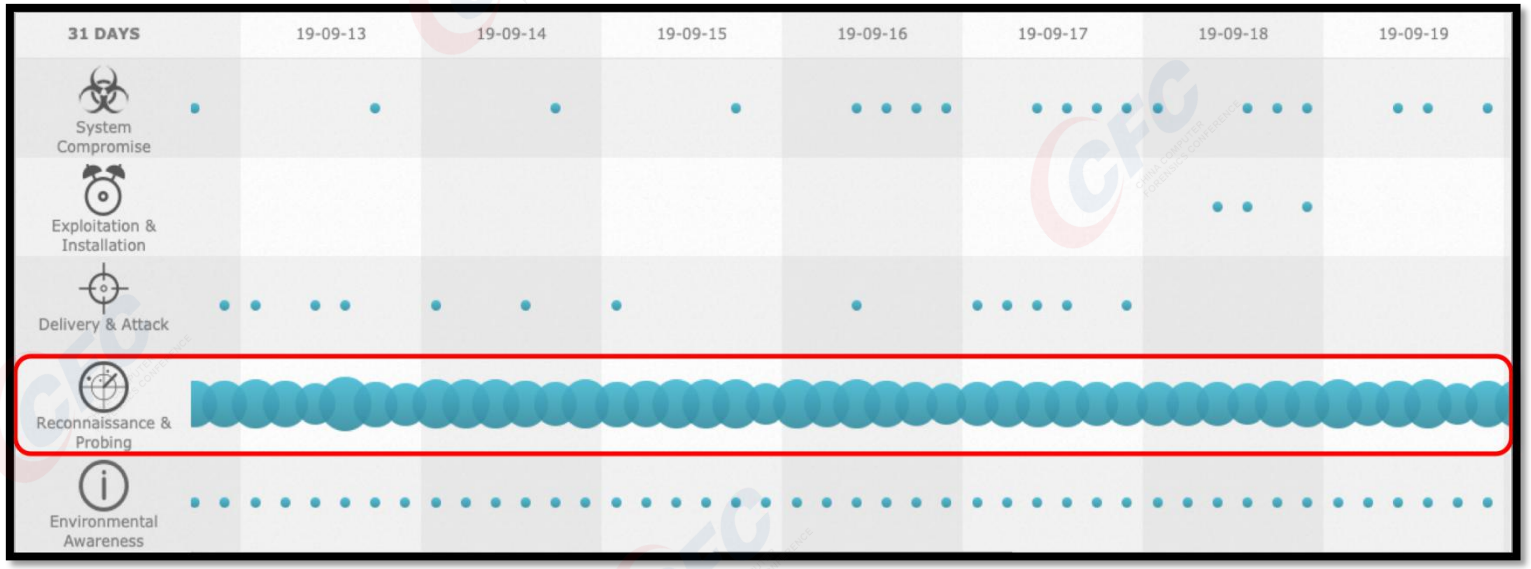
- 相同的恶意代码家族，其灰阶图的样态可能越相似，但并非表示不同的恶意代码家族，其灰阶图的样态便越不相似。
- 虽然透过bytes文件的灰阶图转换，可以在一定程度上帮助辨别恶意代码的家族，但也存在着反例。故仍需透过不同的特征辅助，加以确认其恶意代码家族的特性。

- 特征萃取的品质将间接影响到模型能力的好坏，举例来说，视觉化（bytes文件）和特定关键字之个数（asm文件）等特征，获得了不错的恶意程式家族分类效果。
- 为了得到具有相当功效的分析特征，可以使用集中趋势（Central Tendency）、离散程度（Dispersion）和图像视觉等描述性统计（Descriptive Statistics）方法进行观察，于了解数据特性后订定相关合宜之重要特征。
- 因数据的来源多元且种类繁多，若仅从数据特性的角度去挖掘重要特征并非最佳策略，势必得依赖分析领域的专家知识，才能订定一合适且泛用的重要特征。如此一来，各个特征之间将能相辅相成达到降低误判率之功效，实现恶意代码家族分类之目标。

PART THREE

案例

持续无间断扫瞄弱点漏洞



DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
2019-09-24 11:18:45	open	Portscan	Nmap	LOW (1)	N/A	185.222.211.4:http-proxy	Host-172-16-1-62:1952
2019-09-24 11:18:40	open	Portscan	Nmap	LOW (1)		185.222.211.2:http-proxy	Host-172-16-1-41:tabula
2019-09-24 11:18:02	open	Portscan	Nmap	LOW (1)	N/A	77.247.108.110:53070	Host-172-16-1-211:http
2019-09-24 11:17:32	open	Portscan	Nmap	LOW (1)		141.98.80.219:http-proxy	Host-172-16-1-62:1707
2019-09-24 11:16:29	open	Portscan	Nmap	LOW (1)	N/A	163.172.114.118:http-proxy	Host-172-16-1-62:1331
2019-09-24 11:16:24	open	Portscan	Nmap	LOW (1)	N/A	51.158.25.210:http-proxy	Host-172-16-1-41:1743
2019-09-24 11:15:23	open	Portscan	Nmap	LOW (1)	N/A	193.169.252.64:54984	Host-172-16-1-41:microsoft-ds
2019-09-24 11:14:19	open	Portscan	Nmap	LOW (1)		5.8.18.86:http-proxy	Host-172-16-1-41:1302
2019-09-24 11:13:49	open	Portscan	Nmap	LOW (1)	N/A	78.128.113.84:http-proxy	Host-172-16-1-62:3ds-lm
2019-09-24 11:13:28	open	Portscan	Nmap	LOW (1)		5.189.188.111:56977	Host-172-16-1-35:https

access denied for
155.94.155.250美国QuadraNet
（主机托管及云服务）

荣国

荣国

乌克兰

俄罗斯

保加利亚

德国

恶意挖矿代码攻击

恶意挖矿代码攻击

	2019-09-19 08:41:34	open	Malware infection		CoinMiner	MED (2)	N/A	Host-10-171-8-211:3866	149.28.199.108:https	
1	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2
2	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2
3	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2
4	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2
5	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2
6	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2
7	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2
8	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2
9	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2
10	AlienVault NIDS: "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)"	0	2019-09-19 09:03:35	Host-10-171-8-211:4074	149.28.199.108:https	N/A				2

恶意挖矿代码窃用CPU资源
短时间大量对外连线

```
length = 196

000 : d4 c3 b2 a1 02 00 04 00 00 00 00 00 00 00 00 00   ................
010 : 9c 00 00 00 01 00 00 00 e6 d3 82 5d 2d 48 05 00   ............]-H..
020 : 9c 00 00 00 9c 00 00 00 00 00 00 00 00 00 00 00   ................
030 : 00 00 00 00 08 00 45 00 00 8e 00 00 00 00 00 06   ......E.........
040 : 4a 64 0a ab 08 d3 95 1c c7 6c 0f ea 01 bb 00 00   Jd.......l......
050 : 00 00 00 00 00 00 50 00 00 00 25 5b 00 00 7b 22   ......P...%[..{"
060 : 69 64 22 3a 34 2c 22 6a 73 6f 6e 72 70 63 22 3a   id":4,"jsonrpc":
070 : 22 32 2e 30 22 2c 22 6d 65 74 68 6f 64 22 3a 22   "2.0","method":"
080 : 6b 65 65 70 61 6c 69 76 65 64 22 2c 22 70 61 72   keepalived","par
090 : 61 6d 73 22 3a 7b 22 69 64 22 3a 22 66 37 33 33   ams":{"id":"f733
0a0 : 66 33 36 34 2d 31 34 31 61 2d 34 62 34 63 2d 61   f364-141a-4b4c-a
0b0 : 64 32 61 2d 66 62 39 62 62 37 64 65 33 63 31 64   d2a-fb9bb7de3c1d
0c0 : 22 7d 7d 0a                                       "}}.
```

从数据内容发现挖矿连线痕迹

恶意挖矿代码攻击

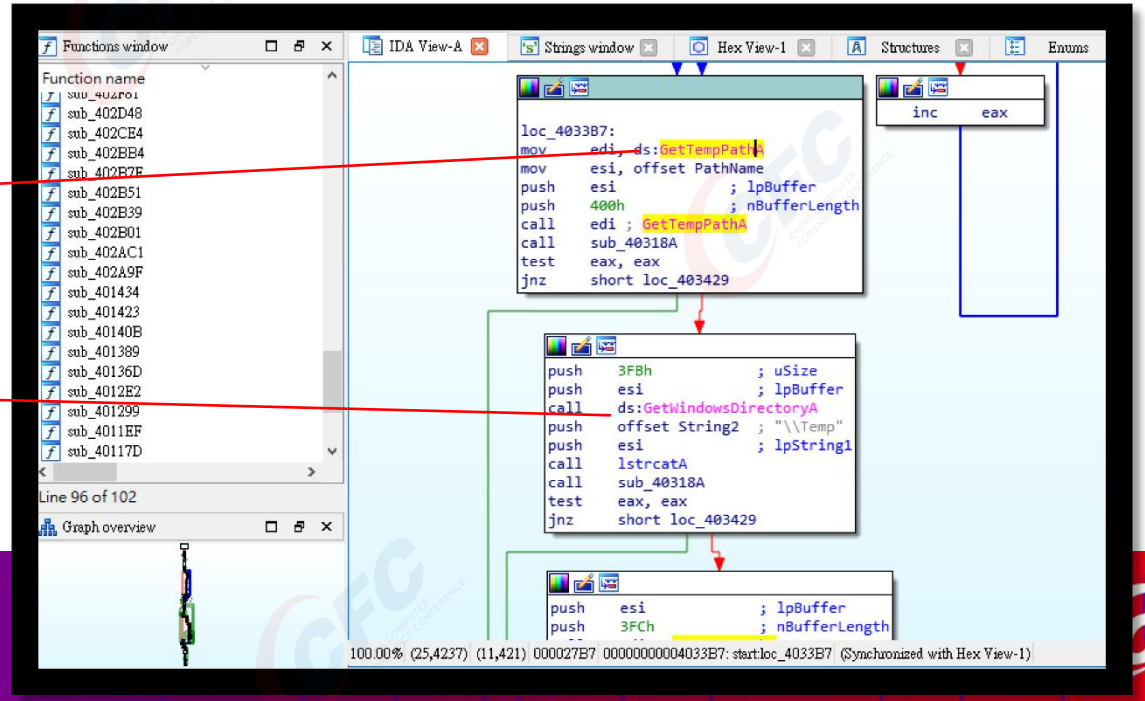
```
push    edi
xor     ebx, ebx
push    8001h           ; uMode
mov     [esp+194h+uExitCode], ebx
mov     [esp+194h+var_184], offset aErrorWritingTe ; "Error writing temporary file. Make sure
mov     [esp+194h+Buffer], ebx
mov     [esp+194h+var_180], 20h
call    ds:SetErrorMode
call    ds:GetVersion
and     eax, 0BFFFFFFFh
cmp     ax, 6
mov     dword_42370C, eax
jz      short loc_40320D

push    ebx
call    sub_4062C7
cmp     eax, ebx
jz      short loc_40320D
```

检索当前进程的错误模式

取得Windows操作系统版本的 API

获取为Temp文件指定的路径

如无新增一个Temp文件夹



恶意挖矿代码攻击

```
call    edi ; GetTempPathA
push    offset aLow     ; "Low"
push    esi             ; lpString1
call    lstrcatA
mov     edi, ds:SetEnvironmentVariableA
push    esi             ; lpValue
push    offset Name     ; "TEMP"
call    edi ; SetEnvironmentVariableA
push    esi             ; lpValue
push    offset aTmp_0   ; "TMP"
call    edi ; SetEnvironmentVariableA
call    sub_40318A
test    eax, eax
jz      loc_4034D7
```

```
loc_403429:             ; lpFileName
push    offset FileName
call    ds:DeleteFileA
push    [esp+194h+Buffer] ; Buffer
call    sub_402D48
cmp     eax, ebx
mov     [esp+194h+var_184], eax
jnz     loc_4034D7
```

更改目前存储处理程序中的环境变数
(将恶意挖矿代码进行隐藏)

```
lea     eax, [esp+190h+TokenHandle]
push    eax             ; TokenHandle
push    28h             ; DesiredAccess
call    ds:GetCurrentProcess
push    eax             ; ProcessHandle
call    ds:OpenProcessToken
push    2
test    eax, eax
pop     edi
jz      short loc_40365E
```

检索当前进程的伪句柄

```
lea     eax, [esp+190h+NewState.Privileges]
push    eax             ; lpLuid
push    offset aSeshutdownpriv ; "SeShutdownPrivilege"
push    ebx             ; lpSystemName
call    ds:LookupPrivilegeValueA
push    ebx             ; ReturnLength
push    ebx             ; PreviousState
lea     eax, [esp+198h+NewState]
push    ebx             ; BufferLength
push    eax             ; NewState
push    ebx             ; DisableAllPrivileges
push    [esp+1A4h+TokenHandle] ; TokenHandle
mov     [esp+1A8h+NewState.PrivilegeCount], 1
```

得到进程的令牌句柄

SQL Injection 攻击

SQL Injection 攻击

#	EVENT	RISK	DATE	SOURCE	DESTINATION	OTX	CORRELATION LEVEL
1	AlienVault NIDS: "ET WEB_SERVER SQL Injection Select Sleep Time Delay"	0	2019-09-24 09:44:31	141.98.81.179:37050	Host-172-16-1-46:http	N/A	3
2	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:29	141.98.81.179:35818	Host-172-16-1-46:http	N/A	3
3	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:27	141.98.81.179:34620	Host-172-16-1-46:http	N/A	3
4	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:23	141.98.81.179:60392	Host-172-16-1-46:http	N/A	3
5	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:22	141.98.81.179:59120	Host-172-16-1-46:http	N/A	3
6	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:20	141.98.81.179:57948	Host-172-16-1-46:http	N/A	3
7	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:18	141.98.81.179:56648	Host-172-16-1-46:http	N/A	3
8	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:16	141.98.81.179:55210	Host-172-16-1-46:http	N/A	3
9	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:15	141.98.81.179:53978	Host-172-16-1-46:http	N/A	3
10	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:13	141.98.81.179:52538	Host-172-16-1-46:http	N/A	3
11	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:11	141.98.81.179:51036	Host-172-16-1-46:http	N/A	3
12	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:09	141.98.81.179:49604	Host-172-16-1-46:http	N/A	3
13	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:07	141.98.81.179:48068	Host-172-16-1-46:http	N/A	3
14	AlienVault NIDS: "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT"	0	2019-09-24 09:44:06	141.98.81.179:46644	Host-172-16-1-46:http	N/A	3

```
050 : 00 00 00 00 00 00 50 00 00 00 fc b7 00 00 47 45   ......P.......GE
060 : 54 20 2f 70 2f 34 31 32 2d 31 30 30 32 2d 33 33   T /p/412-1002-33
070 : 36 2e 70 68 70 3f 4c 61 6e 67 3d 7a 68 2d 74 77   6.php?Lang=zh-tw
080 : 25 32 37 25 32 30 55 4e 49 4f 4e 25 32 30 41 4c   %27%20UNION%20AL
090 : 4c 25 32 30 53 45 4c 45 43 54 25 32 30 4e 55 4c   L%20SELECT%20NUL
0a0 : 4c 25 32 43 4e 55 4c 4c 25 32 43 4e 55 4c 4c 25   L%2CNULL%2CNULL%
0b0 : 32 43 4e 55 4c 4c 25 32 43 4e 55 4c 4c 25 32 43   2CNULL%2CNULL%2C
0c0 : 4e 55 4c 4c 25 32 43 4e 55 4c 4c 25 32 43 4e 55   NULL%2CNULL%2CNU
0d0 : 4c 4c 25 32 43 4e 55 4c 4c 25 32 43 4e 55 4c 4c   LL%2CNULL%2CNULL
0e0 : 25 32 43 4e 55 4c 4c 25 32 43 4e 55 4c 4c 25 32   %2CNULL%2CNULL%2
0f0 : 43 4e 55 4c 4c 25 32 43 4e 55 4c 4c 25 32 43 4e   CNULL%2CNULL%2CN
100 : 55 4c 4c 25 32 43 4e 55 4c 4c 25 32 43 4e 55 4c   ULL%2CNULL%2CNUL
110 : 4c 25 32 43 4e 55 4c 4c 25 32 43 4e 55 4c 4c 25   L%2CNULL%2CNULL%
120 : 32 43 4e 55 4c 4c 2d 2d 25 32 30 53 54 72 70 20   2CNULL--%20STrp
130 : 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74   HTTP/1.1..Accept
140 : 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73   -Language: en-us
150 : 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70   ,en;q=0.5..Accep
160 : 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70   t-Encoding: gzip
170 : 2c 64 65 66 6c 61 74 65 0d 0a 48 6f 73 74 3a 20   ,deflate..Host:
180 : 67 72 61 73 74 75 2e 74 70 61 2e 65 64 75 2e 74   grastu.tpa.edu.t
190 : 77 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f   w..Accept: text/
```

2019-09-14 12:20:22	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	176.121.14.198:53994	Host-172-16-1-46:http	
2019-09-14 00:12:44	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	185.222.209.212:44576	Host-172-16-1-46:http	
2019-09-13 12:59:03	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	176.121.14.179:57968	Host-172-16-1-46:http	
2019-09-13 11:08:43	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	176.121.14.186:45790	Host-172-16-1-46:http	
2019-09-13 02:50:36	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	94.103.9.30:45532	Host-172-16-1-46:http	
2019-09-13 01:30:38	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	141.98.80.95:49750	Host-172-16-1-46:http	
2019-09-12 20:08:44	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	141.98.81.178:38670	Host-172-16-1-46:http	
2019-09-12 11:27:59	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	141.98.81.183:38898	Host-172-16-1-46:http	

俄罗斯

美国QuadraNet

俄罗斯

摩尔多瓦

access denied for
155.94.155.250美国QuadraNet
（主机托管及云服务）

SQL Injection 攻击

```
void
SendResp_albumArt(struct upnphttp * h, char * object)
{
    char header[1500];
    char sql_buf[256];

    /*...abbreviated...*/

    dash = strchr(object, '-');
    if( dash )
        *dash = '\0';
    sprintf(sql_buf, "SELECT PATH from ALBUM_ART where ID = %s", object);
    sql_get_table(db, sql_buf, &result, &rows, NULL);

    /*...abbreviated...*/

}
```

sql_buf放在堆栈上的256字节字符
放入一个无限的sprintf（）中

调用ProcessHttpQuery_unpnphttp（）将长度为512（或更少）字节的字符串发送到SendResp_albumArt（）
堆栈中有一个1500字节的字符数组，sql_buf上方的SendResp_albumArt（），此无法使用而溢出

```
static void
ProcessHttpQuery_upnphttp(struct upnphttp * h)
{
    char HttpCommand[16];
    char HttpUrl[512];
    char * HttpVer;

    /*...abbreviated...*/

    for(i = 0; i<511 && *p != ' ' && *p != '\r'; i++)
        HttpUrl[i] = *(p++);

    /*...abbreviated...*/

    if((strcmp("GET", HttpCommand) == 0) || (strcmp("HEAD", HttpCommand) == 0))
    {
    /*...abbreviated...*/
        else if(strncmp(HttpUrl, "/AlbumArt/", 10) == 0)
        {
            SendResp_albumArt(h, HttpUrl+10);
            CloseSocket_upnphttp(h);
        }

    /*...abbreviated...*/
}
```

SQL Injection 攻击

```
.text:00408F08 loc_408F08:                                  # CODE XREF: SendResp_albumArt+150↑j
.text:00408F08                 la      $a1, 0x430000
.text:00408F0C                 la      $t9, sprintf
.text:00408F10                 addiu   $s0, $sp, 0x750+var_706
.text:00408F14                 addiu   $a1, (aSelectPathFr_0 - 0x430000)  # "SELECT PATH from ALBUM_ART where ID = %"...
.text:00408F18                 move    $a2, $s1
.text:00408F1C                 move    $a0, $s0          # s
.text:00408F20                 jalr    $t9 ; sprintf
.text:00408F24                 move    $s4, $t9
.text:00408F28                 lw      $gp, 0x750+var_738($sp)
.text:00408F2C                 move    $a1, $s0
.text:00408F30                 la      $v0, db
.text:00408F34                 la      $t9, sql_get_table
.text:00408F38                 lw      $a0, (db - 0x47C4A4)($v0)
.text:00408F3C                 addiu   $a2, $sp, 0x750+var_730
.text:00408F40                 sw      $zero, 0x750+var_740($sp)
.text:00408F44                 jalr    $t9 ; sql_get_table
```

验证可执行文件中是否存在SQL injection

勒索病毒攻击

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail wewillhelpyou@qq.com
Write this ID in the title of your message 0665056E-2250
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

勒索病毒攻击

```
8194 call    ds:InternetOpenUrlA
819A mov     edi, eax
819C push    esi             ; hInternet
819D mov     esi, ds:InternetCloseHandle
81A3 test    edi, edi
81A5 jnz     short loc_4081BC

00000000004081BC
00000000004081BC loc_4081BC:
00000000004081BC call    esi ; InternetCloseHandle
00000000004081BE push    edi             ; hInternet
00000000004081BF call    esi ; InternetCloseHandle
00000000004081C1 pop     edi
```

打开由完整的HTTP URL指定的资源

关闭单个Internet句柄

```
00407C84 push    ecx             ; lpBinaryPathName
00407C85 push    1               ; dwErrorControl
00407C87 push    2               ; dwStartType
00407C89 push    10h             ; dwServiceType
00407C8B push    0F01FFh         ; dwDesiredAccess
00407C90 push    offset DisplayName ; "Microsoft Security Center (2.0) Service"
00407C95 push    offset ServiceName ; "mssecsvc2.0"
00407C9A push    edi             ; hSCManager
00407C9B call    ds:CreateServiceA ; Indirect Call Near Procedure
00407CA1 mov     ebx, ds:CloseServiceHandle
00407CA7 mov     esi, eax
00407CA9 test    esi, esi        ; Logical Compare
00407CAB jz      short loc_407CBB ; Jump if Zero (ZF=1)
```

创建服务对象并将其添加到指定的服务控制管理器数据库

关闭服务控制管理器或服务对象的句柄

勒索病毒攻击

```
004020C8 mov     [esp+6F4h+passwordVal], offset aWncry2ol7 ; "WNcry@2ol7"
004020CF push    ebx             ; hModule
004020D0 call    UnzipRsrc       ; Call Procedure
```

使用密码WNcry @ 2ol7提取嵌入式ZIP文件，内容解提取到taskche.exe所在的文件夹中

```
0401EAF push    eax             ; DstBuf
0401EB0 mov     [ebp+Source], offset a13am4vw2dhxygx ; "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
0401EB7 mov     [ebp+var_8], offset a12t9ydpgwuez9n ; "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"
0401EBE mov     [ebp+var_4], offset a115p7ummngoj1p ; "115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn"
0401EC5 call    sub 401000      ; Call Procedure
```

asksche.exe加载比特币钱包地址

勒索病毒攻击

```
4020DC push    offset taskscheCmdline ; "attrib +h ."
4020E1 call    SpawnProcess           ; Call Procedure
4020E6 push    ebx                    ; lpExitCode
4020E7 push    ebx                    ; dwMilliseconds
4020E8 push    offset aIcaclsGrantEve ; "icacls . /grant Everyone:F /T /C /Q"
4020ED call    SpawnProcess           ; Call Procedure
4020F2 add     esp, 20h               ; Add
4020F5 call    LoadLibraries          ; Call Procedure
```

更改zip文件提取到的文件/文件夹的属性
隐藏该文件夹的内容，并向所有用户授予对该文件夹中所有文件的完全访问权限

检测加密密钥提供程序 – Microsoft增强型RSA 和 AES加密提供程序

```
00401833
00401833 loc_401833:
00401833 mov     eax, edi
00401835 push    0F0000000h
0040183A neg     eax                    ; Two's Complemen
0040183C sbb     eax, eax               ; Integer Subtrac
0040183E push    18h
00401840 and     eax, offset aMicrosoftEnhan ; "Mi
00401845 push    eax
00401846 push    0
00401848 push    esi
00401849 call    dword_40F894           ; Indirect Call N
0040184F test    eax, eax               ; Logical Compare
00401851 jnz     short loc_40185C       ; Jump if Not Ze
```

DDoS 攻击

DDoS攻击

攻击来源IP分析

5.252.35.6（美国）	37.59.11.59（德国）	51.68.176.11（荷国）	51.89.191.148（荷国）	54.39.29.72（美国）	66.70.181.31（美国）
80.245.18.71（德国）	71.233.138.232（美国）	74.91.113.64（美国）	93.23.149.229（德国）	109.201.148.62（芬兰）	139.99.28.169（美国）
139.99.125.95（美国）	140.82.56.133（美国）	144.217.62.159（美国）	147.135.36.71（美国）	147.135.91.111（美国）	147.135.119.108（美国）
151.80.230.41（德国）	157.245.10.62（美国）	158.69.5.197（美国）	185.38.151.243（荷国）	185.244.25.187（美国）	188.165.32.190（德国）
193.70.80.122（义大利）					

网络连线在某段时间内，从开始到结束的TCP数据包序列，且在这段时间内数据在协议（例：TCP、UDP）下从来源IP至目的IP的传递。每个网络连接皆会被标记正常或异常，区分异常类型、未知攻击、训练资料等各种攻击手法

加拿大

EVENT NAME	DATE GMT+8:00	SENSOR	OTX	SOURCE	DE	
AlienVault NIDS: "AV DOS Possible Ubiquiti Amplification Scan in Progres S"	2019-09-24 10:59:12	VirtualUSMAllInOne	N/A	142.44.223.235:51570	Host-172-16-1-62:10001	LOW (0)
AlienVault NIDS: "AV DOS Possible Ubiquiti Amplification Scan in Progres S"	2019-09-24 10:59:12	VirtualUSMAllInOne	N/A	142.44.223.235:2049	Host-172-16-1-62:10001	LOW (0)
AlienVault NIDS: "AV DOS Possible Ubiquiti Amplification Scan in Progres S"	2019-09-24 10:59:12	VirtualUSMAllInOne	N/A	142.44.223.235:2286	Host-172-16-1-62:10001	LOW (0)
AlienVault NIDS: "AV DOS Possible Ubiquiti Amplification Scan in Progres S"	2019-09-24 10:59:02	VirtualUSMAllInOne	N/A	142.44.223.235:51570	Host-172-16-1-62:10001	LOW (0)
AlienVault NIDS: "AV DOS Possible Ubiquiti Amplification Scan in Progres S"	2019-09-24 10:59:01	VirtualUSMAllInOne	N/A	142.44.223.235:11535	Host-172-16-1-62:10001	LOW (0)

DST IP ADDRESS	OTX	SENSOR	EVENTS # (*)	UNIQUE EVENTS	UNIQUE SRC. CONTACTED.	GEO TOOLS
172.16.1.62	N/A	VirtualUSMAllInOne - 10.171.2.52	73,871	1	1,254	
172.16.1.41	N/A	VirtualUSMAllInOne - 10.171.2.52	48	1	28	

CFC
CHINA COMPUTER
FORENSICS CONFERENCE

THANKS FOR YOUR WATCHING

CONTACT ME

联系方式：

电话：13215943436

邮件：chang.pie@gmail.com

微信：chang_pie

Q Q：2912111476