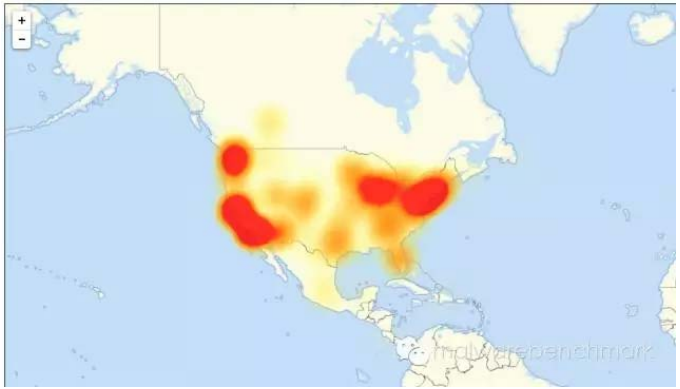
从恶意代码基因看物联网安全防护

Pr0.s 单征

美国东部断网事件



10月21日，一场始于美国东部的大规模互联网瘫痪席卷全美。众所周知的原因是以迪恩和亚马逊为代表的网络服务提供商，遭受了，受Mirai等恶意代码控制的号称“百万”物联网设备的DNS攻击。

周三，美国东部再次断网。

MalwareBenchmark早在10月5日就发出了互联网可能发生大规模DoS攻击的警告，并在9月发布了BashLite家族的分析报告，10月9日、11日发布了Mirai的分析报告，但灾难还是发生了

之后… …世界多地发生多起类似事件

继而，新加坡StarHub（星和）、我国的北京XX、XXX、XX等也受到了此类攻击，流量超500G。本月24日，欧盟委员会再遭攻击断网。

以华为海思芯片及相关主板的海康威视、大华、雄迈等厂商产品是主要受害者，甚至包括：华为和中兴打印机、路由器。

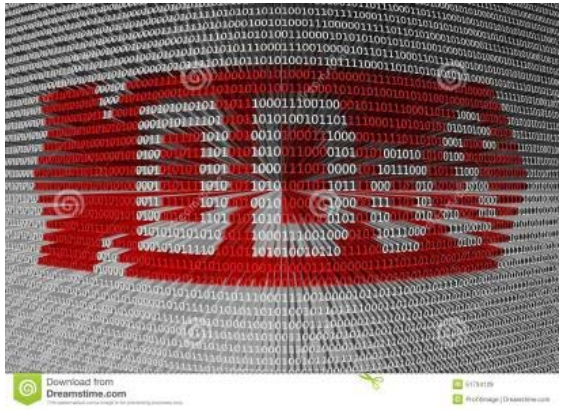
境内已查证受控设备远超10万台。

控制物联网设备的恶意代码包括：Mirai、Lizkebab, BASHLITE, Torlus, Gafgyt、Luabot、DYREZA、AppleJ4ck、CCTV、肉鸡MM、BillGates、Mayday、PNScan、Remaiten等种类；

同源性明显，例如Lizkebab, BASHLITE, Torlus, Gafgyt等源自ShellLock；

针对物联网设备的新型变种病毒快速增长，例如Hajime。

之后… …新型网络犯罪模式



受控设备类型多样，百万台；1次攻击流量可超1Tbps；

利用漏洞包括：弱口令、SSHowDowN Proxy、Bash Shell后门等；

部分恶意代码兼具传播、渗透功能，可以加载更多的功能模块；例如Mirai的load模块提供了用户可定制的功能，DYREZA恶意代码能够通过路由器传播大量的渗透工具。

DDoS攻击的方式本身没有改变

黑客寻找到了新的模式

如同：Malware-as-Service、Ransomware-as-Service

而开放源代码犹如打开了“潘多拉盒子”，加速了这一过程

Mirai家族的影响

受控设备已经遍布全球164 个国家，越南占据榜首 12.8%，其后是巴西在11.8%，美国 10.9%，中国 8.8%和墨西哥，8.4%。韩国、 台湾、 俄罗斯、 罗马尼亚和哥伦比亚等十个国家受影响最严重。黑山、 塔吉克斯坦和索马里等偏远地区也未能“豁免”；

目前物联网受控设备包括Web服务器、路由器、调制解调器、网络连接存储（NAS）设备、闭路电视（CCTV）系统和工业控制系统等种类，数目超过百万；

Mirai境内分布

Mirai主控服务器分布

Mirai的升级Rakos

Rakos恶意软件通过GO语言编写，采用标准的UPX加壳。Rakos通过标准输入加载其配置，配置文件的格式为YAML。配置文件中包含CC服务器，弱口令配对，内部参数等。

该bot的特点是，扫描的IP不是类似于Mirai的随机产生，而是通过https://{C&C}/scan来指定，不过该列表的更新速度非常快。

HTTP连接http://127.0.0.1:61314，通过http://127.0.0.1:61314/et的ET请求来终止任意进程，通过http://127.0.0.1:61314/ex请求来解析一些url请求。

之后… …国际

11月15日，美国发布的“保障物联网安全的战略原则，版本1.0”中，美国国土安全部（DHS）表示，物联网制造商必须在产品设计阶段构建安全，否则可能会被起诉。

11月16日，物联网IoT安全性的美国会听会上，众议员Greg Walden、Anna Eshoo、Fu等纷纷发言

在所有利益相关者中构建与物联网有关的风险意识（明确向厂家提供不安全产品的后果，这个值得深切关注）

网络安全测试

联邦政府资助独立实验室和一个全新的联邦机构致力于网络安全

为物联网国际标准发展进程做贡献。（抢占安全标准制高点）

物联网网络安全威胁的新源头？

物联网网络空间（CyberSpace）的重要组成部分

美国发布的“保障物联网安全的战略原则，版本1.0”中，美国国土安全部（DHS）表示，物联网制造商必须在产品设计阶段构建安全，否则可能会被起诉。

由网络安全政策与法律联盟（Coalition for Cybersecurity Policy and Law）举办的下一任总统网络安全研讨会上，DHS部长杰伊•约翰逊(Jeh Johnson)甚至表示，“美国无法承受来自物联网安全威胁的后果，保障物联网安全已演变为国土安全问题”。

物联网网络安全威胁的新源头？

物联网设备和网络，大部分时间涉及HMI较少，成为网络空间安全领域的”死角 “

物联网面临着与互联网同样的安全威胁

物联网安全由于长期受到忽视，急需补课

新源头不是原理层面　　更多是管理层面

来自白银杀人案侦破的启示

由指纹到基因

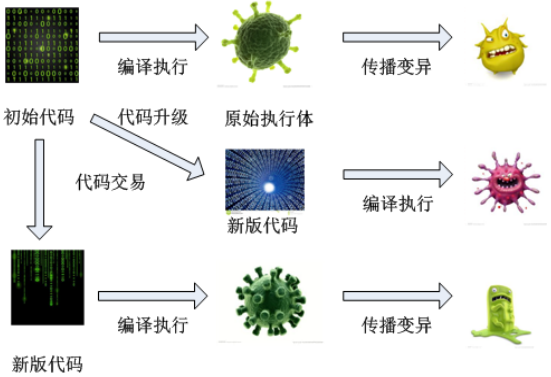
极大提升刑侦效率

生物基因技术在刑事侦查、疾病诊疗、物种改良等领域的广泛应用，使得以往这些工作效果和效率提升了数十倍乃至数百倍，这缘于基因技术从分子视角对物种的精确认识。

高速衍生进化——安全威胁日益复杂严峻

网络空间内恶意病毒、木马，乃至软件和信息是在于网络空间内软硬件等各类环境不断对抗和适应过程中的得以复制和传播的，与生物物种的繁衍和进化有着非常相似的内在机制和过程。

不同的是，在网络空间这一“人造世界”，软件和信息产生、进化和消亡的周期与速度更为快速，且呈非几何速度递增。



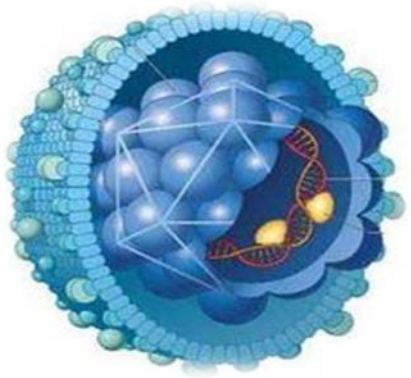
化繁为简——软件基因的分析与利用

正如近百年人类从“基因”视角认知、分析、利用，甚至改造生物体的研究工作方法。

将多样性、复杂性，拆分简约成相对抽象、简一的研究对象。

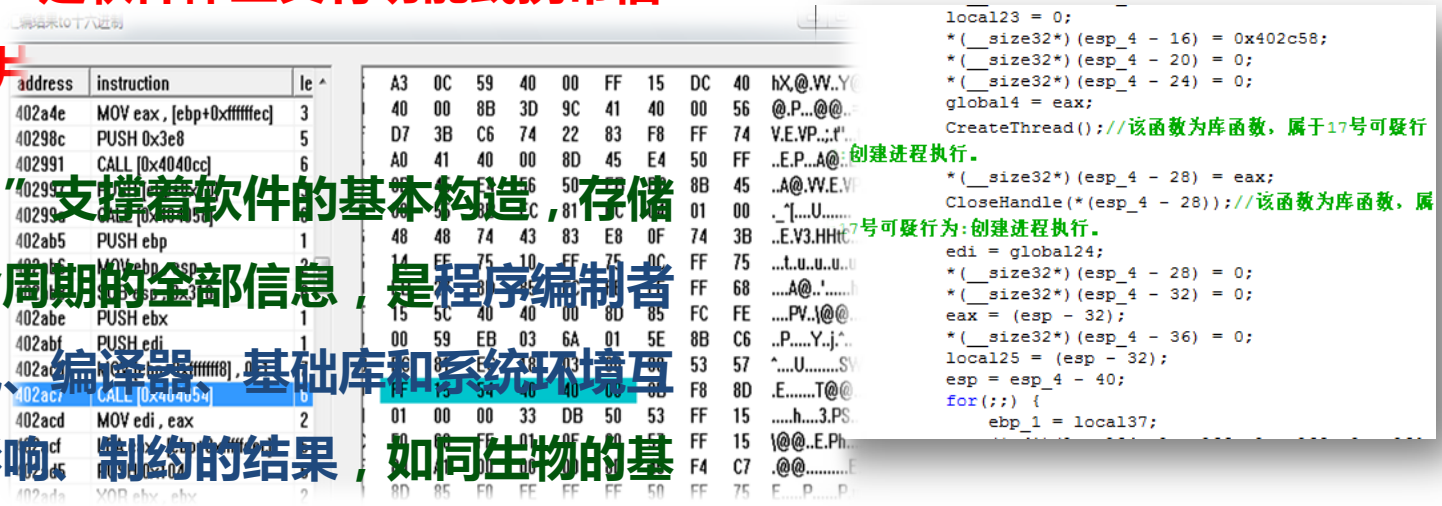
我们的思路：

推论猜测+个体验证+群体分析+功能拆解+应用研究



软件基因——具有双重属性的基本组成

“软件基因”是软件体上具有功能或携带信息的二进制片



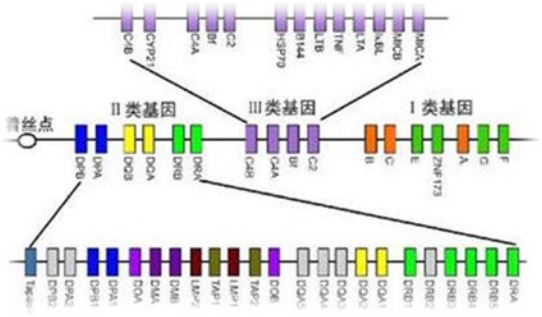
“软件基因”支撑着软件的基本构造，存储着软件生命周期的全部信息，是程序编制者的语义实现、编译器、基础库和系统环境互相依赖、影响、制约的结果，如同生物的基因，具有双重属性：物质性和信息性。

基因组——支撑独立功能的基因序列

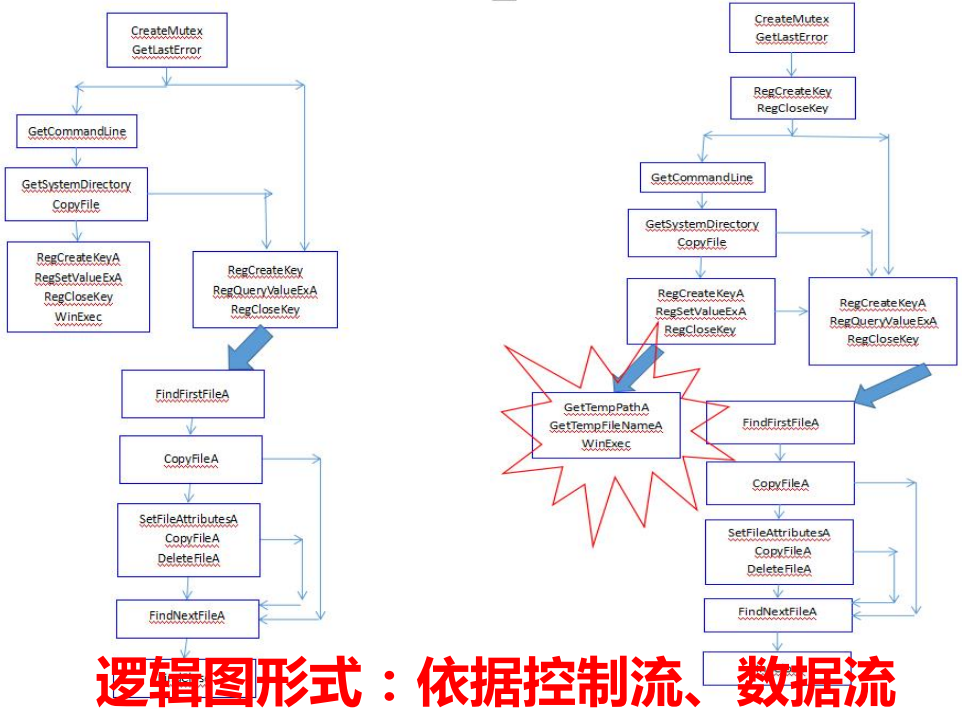
软件基因组，一个软件所携带的一套完整的基因序列，包括全套基因和间隔序列，一个软件的基因组可以标识出唯一的一个软件体。

软件行为基因组，一套支撑某种软件行为的基因序列，一套行为基因组可以独立支撑某项软件功能或行为。

特定行为基因组内，某些基因可以顺序无关。



基因组分析——逻辑与物理两种表示形式

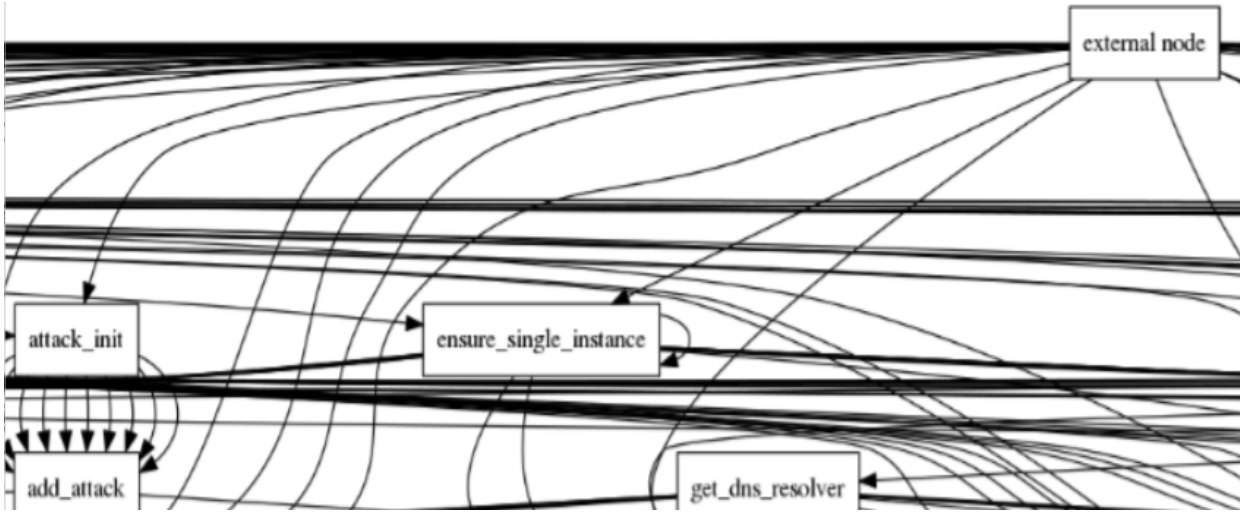


逻辑图形式：依据控制流、数据流
用于种族分析

00409000	RegCreateKeyA
00409004	RegCloseKey
00409008	RegQueryValueExA
0040900C	RegSetValueExA
00409014	WinExec
00409018	GetTempFileNameA
0040901C	FindFirstFileA
00409020	CopyFileA
00409024	FindNextFileA
00409028	GetCommandLineA
0040902C	GetLastError
00409030	CreateMutexA
00409034	SetFileAttributesA
00409038	DeleteFileA
0040903C	GetTempPathA
00409040	GetSystemDirectoryA
00408000	RegCreateKeyA
00408004	RegSetValueExA
00408008	RegQueryValueExA
0040800C	RegCloseKey
00408014	WinExec
00408018	FindFirstFileA
0040801C	CopyFileA
00408020	FindNextFileA
00408024	GetLastError
00408028	CreateMutexA
0040802C	SetFileAttributesA
00408030	DeleteFileA
00408034	GetSystemDirectoryA
00408038	GetCommandLineA

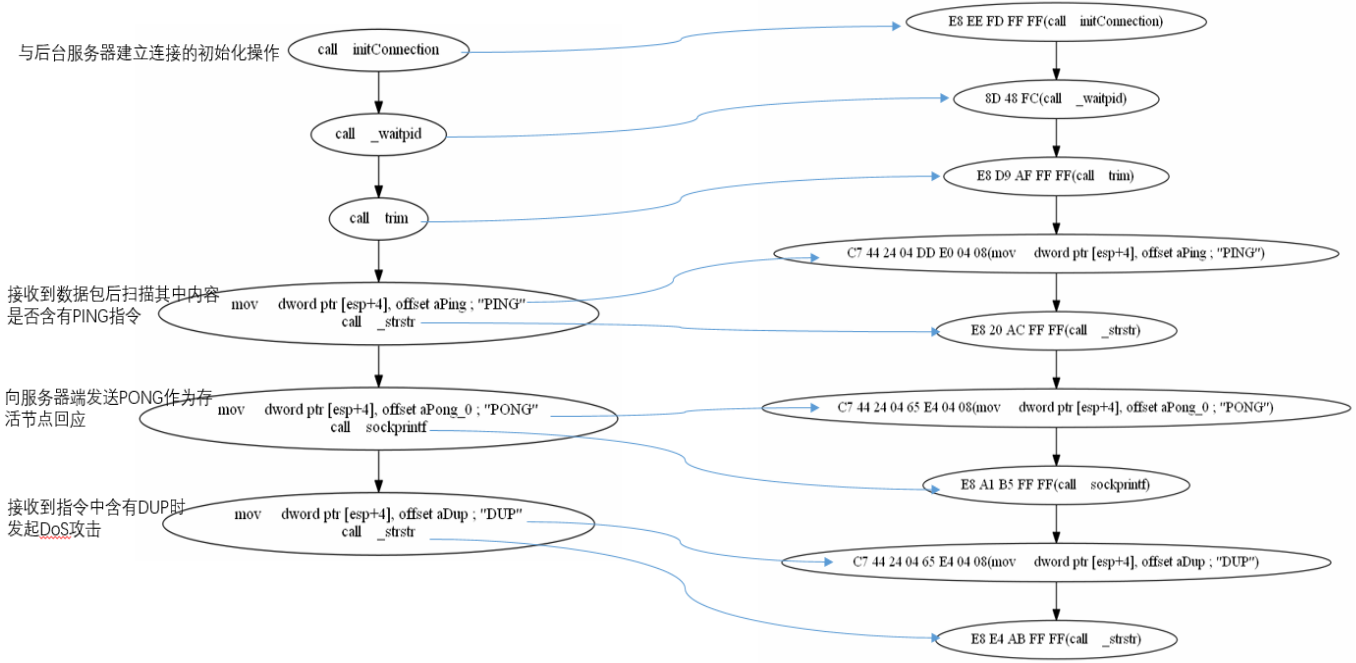
物理链形式：依据文件二进制、存储
用于处理识别

基因组——支撑独立功能的基因序列



Mirai ' Gene

相关恶意代码家族的基因检测与识别



Bashlite家族衍生进化与网络通信基因

相关恶意代码家族图谱

Aidra

2013年第一代IRCtelnet，利用弱口令感染IOT设备

Torlus　Gayfg

2014年出现引入linux跨平台特性和TelnetScancer

Lizkebab

Bathlite

2016年改进型僵尸网络，控制设备首次超百万

Miria

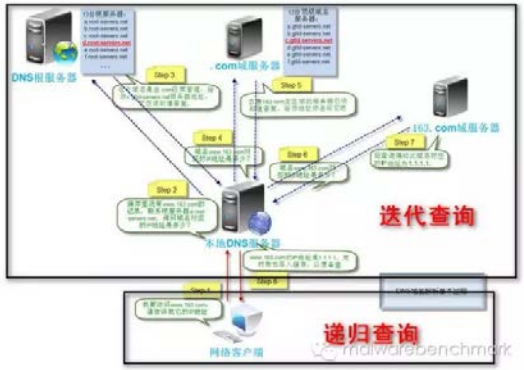
开放源代码，独占设备，攻击方式多样，危害巨大

Hajime　BrickerBot

Rakos

针对SSH Scancer

原因分析一：DNS的脆弱性



DNS脆弱性的本质：

1）DNS服务的公开性。2）DNS访问的匿名性。3）DNS查询的复杂性。（Bind 2万-3万； Route53 50万）

大规模DDoS攻击的难度：

1）控制协同难。2）经济代价高。3）时间成本高。

黑客目的和诉求 值得思考而卡巴斯基的研究人员，则分析：近期，DDoS 事件频率、 规模和复杂度呈现上升态势。罪犯正在越来越多地使用这些攻击作为"烟幕弹"，转移对其真正攻击意图的公众和技术人员注意力。

MalwareBenchmark在10月24日发表文章“搞掉美国东部网络用得着百万设备吗？”，经估算参与攻击设备10万台左右。

两天后，Dyn等官方确认参加攻击设备10万台

原因分析二：物联网设备的安全机制缺失

物联网面临的威胁源头、本质：

1）管理疏忽，无专业人员运维。

2）企业忽视，成本压力大。

3）缺乏自主创新，技术陈旧。

大多数物联网设备不在保密、等保等政策和法规要求范围之内，业务领域缺乏政策引导和监督，也没有规模化专业安全企业提供相关服务。

物联网及其应用已经深入渗透社会的方方面面，与能源、交通、金融等国家关键基础设施、智慧城市中的人民生活、党政军核心部门的管理运营等紧密相关，是网络空间的重要组成部分，其安全威胁不容小觑，造成的影响，有可能更甚于传统安全领域。

相关建议一：物联网设备的安全机制建设

（1）加强政策引导和监督。

加强相关法规建设；在重点行业、区域、领域实施审查和准入制；加强相关管理运维制度建设；在相关领域建立合适的奖励激励机制；



相关建议二：物联网设备的安全机制建设

（2）成立相关机构或部门。

加强物联网安全领域专业的执法监督、应急响应、测评、测试、咨询、监理机构建设；建设物联网领域高效合理的安全事件通报和应急响应机制、体系；构建物联网领域的CA体系；与其它国家和境外企业、用户建立国际协同的通报、预警、防御和响应机制；

相关建议三：物联网设备的安全机制建设

（3）加强相关技术手段建设。

加强相关物联网安全标准和基线建设；建设国家级物联网态势感知系统；建设物联网安全领域靶场和试验床；

同时，基于上述政策、机构和技术手段支撑，开展物联网安全的专业化常态化检查评估；安全事件实时分析、通报、监控及预警；引导和指导相关机构和厂商开展核心技术攻研，协同用户安全防御；扶持相关专业安全厂商与服务队伍；开展相关知识的宣讲和人员培训… …等工作。

相关建议四：物联网设备的安全机制建设

在美国断网事件后，美国国土安全部、欧盟委员会等纷纷表示要近期出台或加强原有相关领域的法规和政策。由此，能否引起对中国产相关产品的限制性销售或加强审核，构建贸易“壁垒”值得关注。

同时，建议做好舆论准备和积极应对策略。

另外，海思芯片的ARM架构，兼容目前互联网恶意代码，对于国产自主可控的范畴，值得思考。

另：恶意代码认知、分类、命名研究

事件通报，统一命名

致乌克兰电网事件的恶意代码样本，至今为止，安全企业给出的命名和描述多达十几种

本质是对安全事件缺乏统一的认知

语义、正则、可识别

…… ……

McAfee-GW-Edition	BehavesLike.Win32.PWSZbot.mm	20160916
eScan	Gen:Variant.BlackEnergy.13	20160916
Microsoft	Trojan:Win32/Dynamer!ac	20160916
NANO-Antivirus	Trojan.Win32.KillFiles.dygjox	20160916
Panda	Trj/GdSda.A	20160915
Qihoo-360	HEUR/QVM09.0.Malware.Gen	20160916
Rising	Trojan.KillDisk!1.A38A (classic)	20160916
Sophos	Troj/Defkill-A	20160916
Symantec	Trojan.Disakil	20160916
Tencent	Win32.Trojan.Cryfile.Syrq	20160916
TheHacker	Trojan/KillDisk.nbc	20160916
TrendMicro	TROJ_KILLDISK.C	20160916
TrendMicro-HouseCall	TROJ_KILLDISK.C	20160916
VBA32	Trojan.KillFiles	20160915
VIPRE	Trojan.Win32.Generic!BT	20160916
ViRobot	Trojan.Win32.Z.Killdisk.90112[h]	20160916
Yandex	Trojan.CryFile!905dgDbIRqQ	20160915
Zillya	Trojan.KillDisk.Win32.176	20160915
nProtect	Trojan/W32.CryFile.90112	20160916
Alibaba	✔	20160914

另：未来工作——探索安全评测基准

安全基线，量化评测

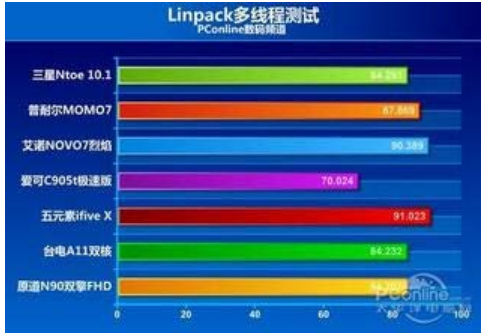
“等保”等过于定性，安全界缺乏定量的基线

攻击性测试，非商业化行为，行业标准

构建开放、开源、众测平台体系和基准测试

NGO and WorkGroup

… …



Linpack

MalwareBenchmark

工控——安全——法律法规、技术标准规范

网络安全立法

应具技术前瞻性

信息泄露——威胁源头、减少暴漏面

信息共享——信息发布/共享机制、范围

等保分保——分级分域、成熟模式

检测评估——设备、体系、验收、事故调查

应急响应——预案、队伍、技术工具

培训认证——人员意识、技术能力、岗位认证

数据留存——取证依据

自主可控——安全基础

体制、政策、机制激励——可实施

敬请批评指正！

9.18 临安中都青山湖畔大酒店见~！