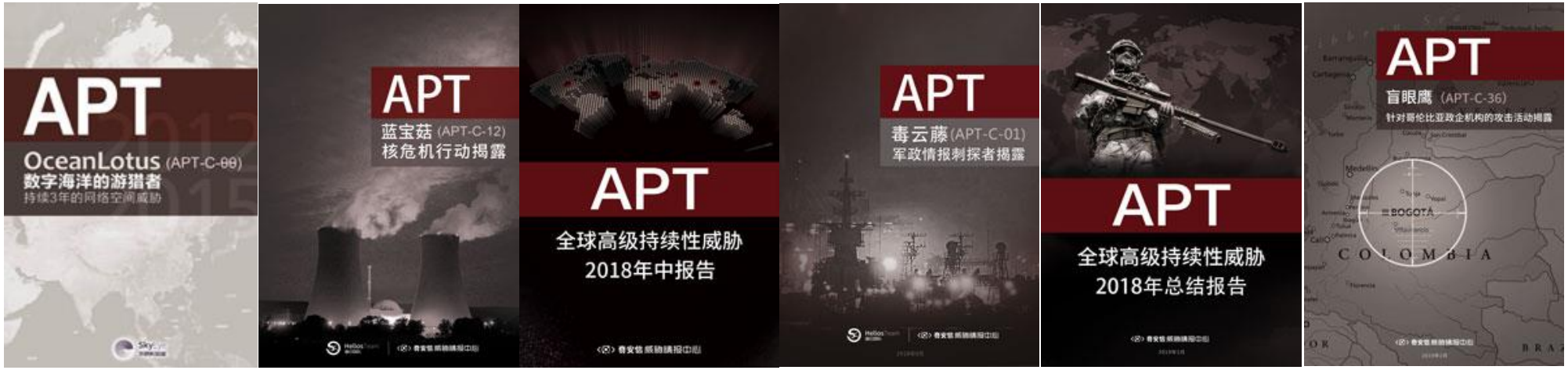
基于ATT&CK的APT威胁跟踪和狩猎

潘博文　奇安信威胁情报中心

团队介绍

- 奇安信威胁情报中心 – “红雨滴”团队
- 奇安信下专注于威胁情报方向和高级威胁分析的团队
- 主要方向为定向攻击事件和高级威胁分析、发现和响应，机读威胁情报的生产和输出
- 曾发现和披露数个APT组织，并长期跟踪活跃APT组织活动



目录

兵者，诡道也

图片来源网络

MITRE

ATT&CK™

STIX™

TTP in STIX 1.2

TTP	
ID	example:ttp-dd955e08-16d0-6f08-5064-50d9e7a3104d
Title	Malware C2 Channel
Resources	
Infrastructure	
Type	Malware C2 (None)
Observable_Characterization	
Observable	
idref	example:observable-c8c32b6e-2ea8-51c4-6446-7f5218072f27
Observable	
idref	example:observable-b57aa65f-9598-04fb-a9d1-5094c36d5dc4
Observable	
idref	example:observable-19c16346-0eb4-99e2-00bb-4ec3ed174cac

https://stixproject.github.io/documentation/idioms/c2-ip-list/

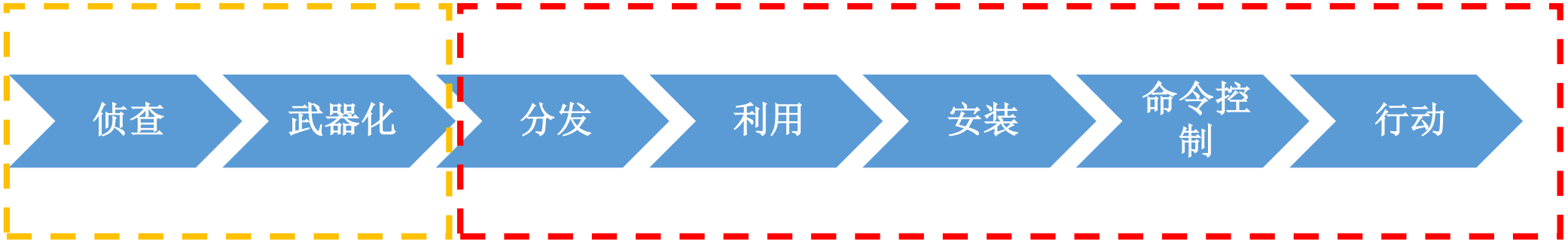
Attack Pattern in STIX 2.0

Phishing
external_references: [{
source_name: capec,
description: phishing,
url: https://capec.mitre.org...,
external_id: CAPEC-98 }]
kill_chain_phases [{
kill_chain_name: mandiant-attack-lifecycle-model,
phase_name: initial-compromise

ATT&CK 映射到STIX 2.0


```
"objects": [
    {
        "external_references": [
            {
                "url": "https://attack.mitre.org/techniques/T1033",
                "source_name": "mitre-attack",
                "external_id": "T1033"
            },
            {
                "url": "https://capec.mitre.org/data/definitions/577.html",
                "source_name": "capec",
                "external_id": "CAPEC-577"
            }
        ],
```

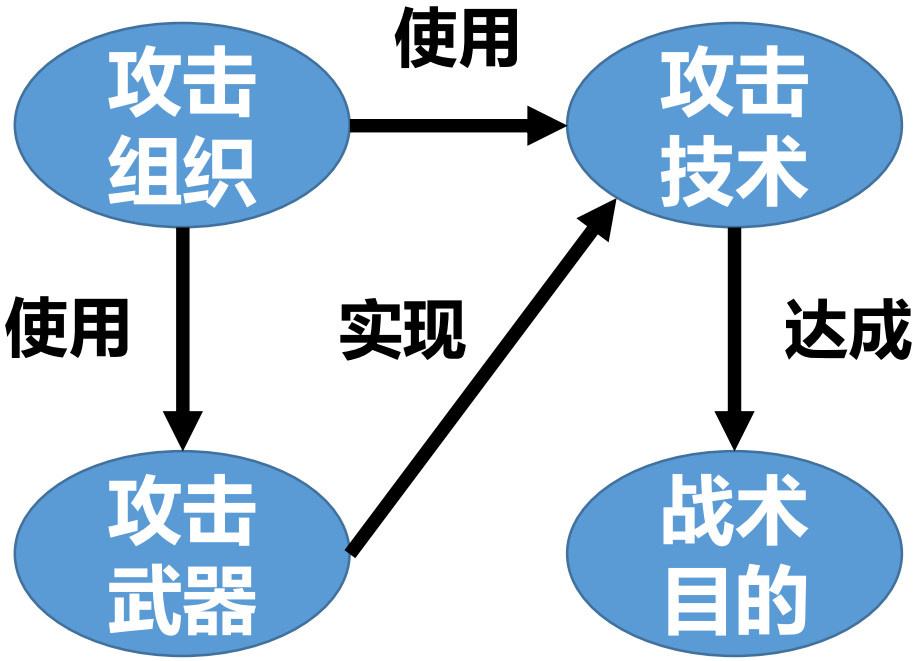
PRE-ATT&CK **Enterprise**



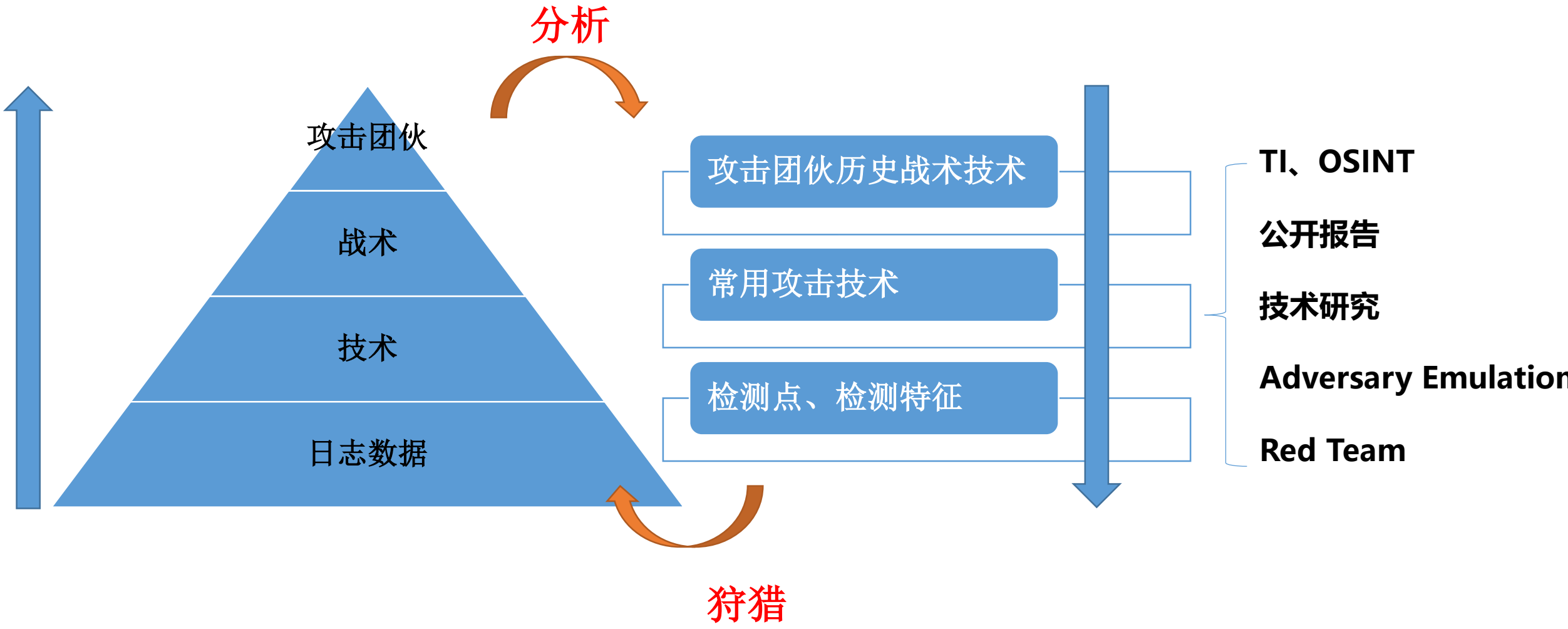
初始进入	代码执行	持久性	权限提升	防御绕过	凭据获取	内部探测	横向移动	信息收集	数据窃取	命令控制	影响
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Logon Scripts	Data from Information Repositories	Data Encoding	Data Transfer Size Limits	Disk Content Wipe
Spearphishing via Service	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Local System	Data Obfuscation	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Supply Chain Compromise	Execution for Client Execution	Authentication Package	Bypass User Account Control	CMSTP	Exploitation for Credential Access	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Domain Fronting	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Trusted Relationship	Graphical User Interface	BITS Jobs	DLL Search Order Hijacking	Code Signing	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Generation Algorithms	Exfiltration Over Physical Medium	Firmware Corruption
Valid Accounts	InstallUtil	Bootkit	Dylib Hijacking	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Data Staged	Fallback Channels	Scheduled Transfer	Inhibit System Recovery
	LSASS Driver	Browser Extensions	Exploitation for Privilege Escalation	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Email Collection	Multi-hop Proxy		Network Denial of Service
	Mshta	Change Default File Association	Extra Window Memory Injection	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Input Capture	Multi-Stage Channels		Resource Hijacking
	PowerShell	Component Firmware	File System Permissions Weakness	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Man in the Browser	Multiband Communication		Runtime Data Manipulation
	Regsvcs/Regasm	Component Object Model Hijacking	Hooking	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Query Registry	Taint Shared Content	Screen Capture	Multilayer Encryption		Service Stop
	Regsvr32	Create Account	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Network Sniffing	Remote System Discovery	Third-party Software	Video Capture	Remote Access Tools		Stored Data Manipulation
	Rundll32	DLL Search Order Hijacking	New Service	Disabling Security Tools	Password Filter DLL	Security Software Discovery	Windows Admin Shares		Remote File Copy		Transmitted Data Manipulation
	Scheduled Task	External Remote Services	Path Interception	DLL Search Order Hijacking	Private Keys	System Information Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Scripting	File System Permissions Weakness	Port Monitors	DLL Side-Loading	Two-Factor Authentication Interception	System Network Configuration Discovery			Standard Cryptographic Protocol		
	Service Execution	Hidden Files and Directories	Process Injection	Execution Guardrails		System Network Connections Discovery			Standard Non-Application Layer Protocol		
	Signed Binary Proxy Execution	Hooking	Scheduled Task	Exploitation for Defense Evasion		System Owner/User Discovery			Uncommonly Used Port		
	Signed Script Proxy Execution	Hypervisor	Service Registry Permissions Weakness	Extra Window Memory Injection		System Service Discovery			Web Service		
	Third-party Software	Image File Execution Options Injection	SID-History Injection	File Deletion							
	Trusted Developer Utilities	Logon Scripts	Valid Accounts	File Permissions Modification							
	User Execution	LSASS Driver	Web Shell	File System Logical Offsets							
	Windows Management Instrumentation	Modify Existing Service		Group Policy Modification							
	Windows Remote Management	Netsh Helper DLL		Hidden Files and Directories							
	XSL Script Processing	New Service		Image File Execution Options Injection							
		Office Application Startup		Indicator Blocking							
		Path Interception		Indicator Removal from Tools							
		Port Monitors		Indicator Removal on Host							
		Redundant Access		Indirect Command Execution							
		Registry Run Keys / Startup Folder		Install Root Certificate							
		Scheduled Task		InstallUtil							
		Screensaver		Masquerading							
		Security Support Provider		Modify Registry							
		Service Registry Permissions Weakness		Mshta							
		Shortcut Modification		Network Share Connection Removal							
		SIP and Trust Provider Hijacking		NTFS File Attributes							
		System Firmware		Obfuscated Files or Information							
		Time Providers		Process Doppelgänging							
		Valid Accounts		Process Hollowing							
		Web Shell		Process Injection							
		Windows Management Instrumentation Event Subscription		Redundant Access							
		Winlogon Helper DLL		Regsvcs/Regasm							
				Regsvr32							
				Rootkit							
				Rundll32							
				Scripting							
				Signed Binary Proxy Execution							
				Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

战术目的

技术实现



数据与处理 - ATT&CK


分析
攻击团伙
战术
技术
日志数据
攻击团伙历史战术技术
常用攻击技术
检测点、检测特征
TI、OSINT
公开报告
技术研究
Adversary Emulation
Red Team
狩猎

数据与处理 - ATT&CK

- WINDOWS日志
- SYSMON
- AUTORUNS
- 自定义的终端网络行为监测程序
- 自定义的系统行为监测程序

ID: T1086

Tactic: Execution

Platform: Windows

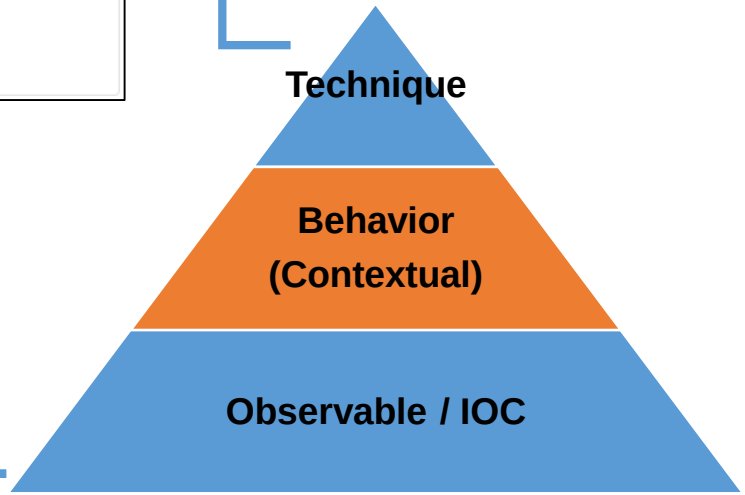
Permissions Required: User, Administrator

Data Sources: PowerShell logs, Loaded DLLs, DLL monitoring, Windows Registry, File monitoring, Process monitoring, Process command-line parameters

Supports Remote: Yes

Contributors: Praetorian

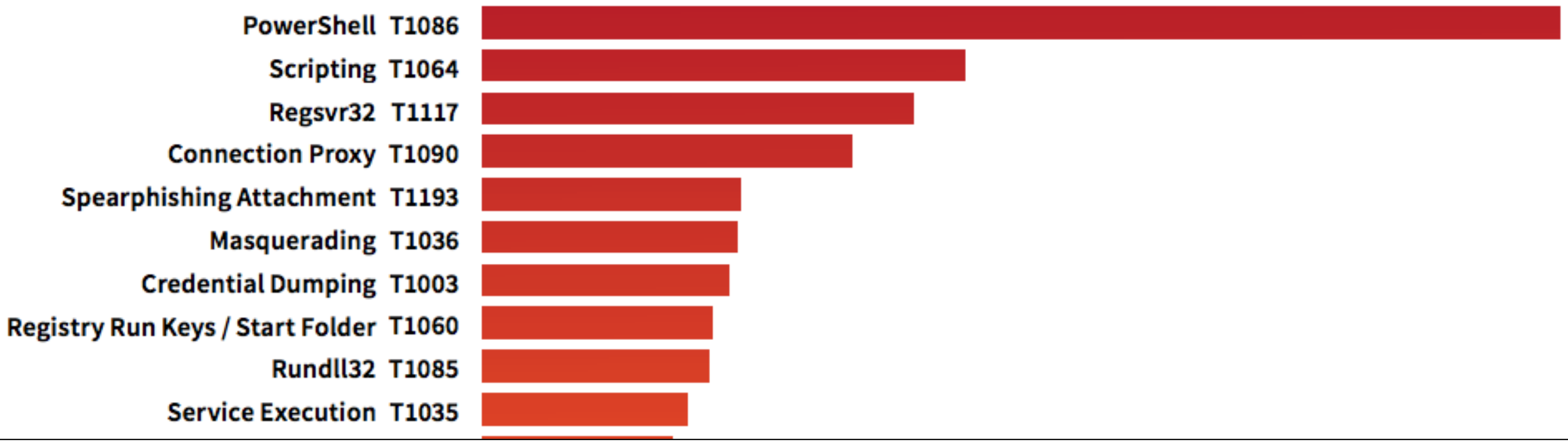
Version: 1.1



战术与技术

- ATT&CK
  - Enterprise Techniques：覆盖Windows、Linux、MacOS，涉及244项攻击技术
  - Groups：覆盖了公开活跃的APT组织或黑客团伙86个
  - Software：覆盖了常用恶意代码、攻击工具或系统工具377个

战术与技术



Red Canary “Threat Detection Report” 2019
https://resources.redcanary.com/hubfs/ThreatDetectionReport-2019.pdf

系统API

- CreateProcessA() and CreateProcessW(),
- CreateProcessAsUserA() and CreateProcessAsUserW(),
- CreateProcessInternalA() and CreateProcessInternalW(),
- CreateProcessWithLogonW(), CreateProcessWithTokenW(),
- LoadLibraryA() and LoadLibraryW(),
- LoadLibraryExA() and LoadLibraryExW(),
- LoadModule(),
- LoadPackagedLibrary(),
- WinExec(),
- ShellExecuteA() and ShellExecuteW(),
- ShellExecuteExA() and ShellExecuteExW()

一些实现方式

Create Process Using Temp Directory (LoadFromDisk_GHR - Gharial) SECRET

Create A Process Via COM Class Creation (COMLocalServerRun_SHTA - Shasta) SECRET

Create Process And Choose A User To Run As Via The Task Scheduler (TaskSchedulerRun_SPKL - Speckled) SECRET

Create Process Via ShellExecute (ShellExecute_CRS - Chorus) SECRET

Create Process Using WMI (CreateProcessWMI_TIG - Tiger) SECRET

Create Process And Pipe The Results (CreateProcessPipe_GHRN - Greenhorn) SECRET

Create Process As Current User +Admin (CreateProcessAsUser_LEP - Leopard) SECRET

Create Process (CreateProcess_SPF - Spadefoot) SECRET

regsvr32,rundll32,mshta,powershell,wmic,psexec, …

APT组织对公开工具的使用

Cobalt Strike, beacon	many actors, like Oceanlotus
Invoke-PSImage	Olympic Destroyer
Powershell Empire	Olympic Destroyer, WIRTE
Metasploit, meterpreter	some actors, like Turla, DarkHydrus
BeEF	Winnti Umbrella, Charming Kitten
Koadic	APT28
Fuzzbunch	Leafminer
Phishery	DarkHydrus
fingerprintjs2	Oceanlotus
Responder	TEMP.Periscope
Crackmapexec	MuddyWater
LaZagne	MuddyWater
Mimikatz	many actors
Windows Credential Editor	APT39, APT40
AdFind	FIN6
DKMC	Oceanlotus

技术盗用

Component Library

The UMBRAGE team maintains a library of application development techniques borrowed from in-the-wild malware. The combined into custom solutions. Rather than building feature-rich tools, which are often costly and can have significant C to operational specifications.

This page organizes this collection based on its functionality and captures relevant technical information. When possible, code in the SVN repository), documentation describing application of the technique, and notes concerning our use of these

The Umbrage Component Library git repository (located in Stash) contains example code for many of these techniques.

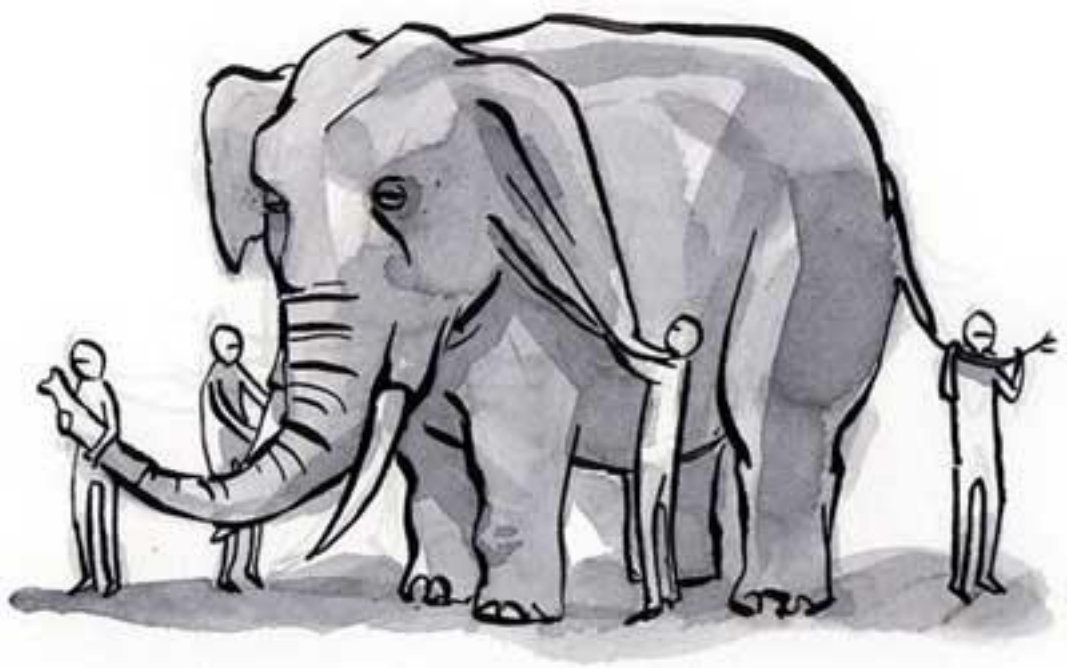
- 数据收集
- 数据擦除
- 持久化
- 权限提升
- 隐藏
- 反AV/反调试/反RE
- 探测

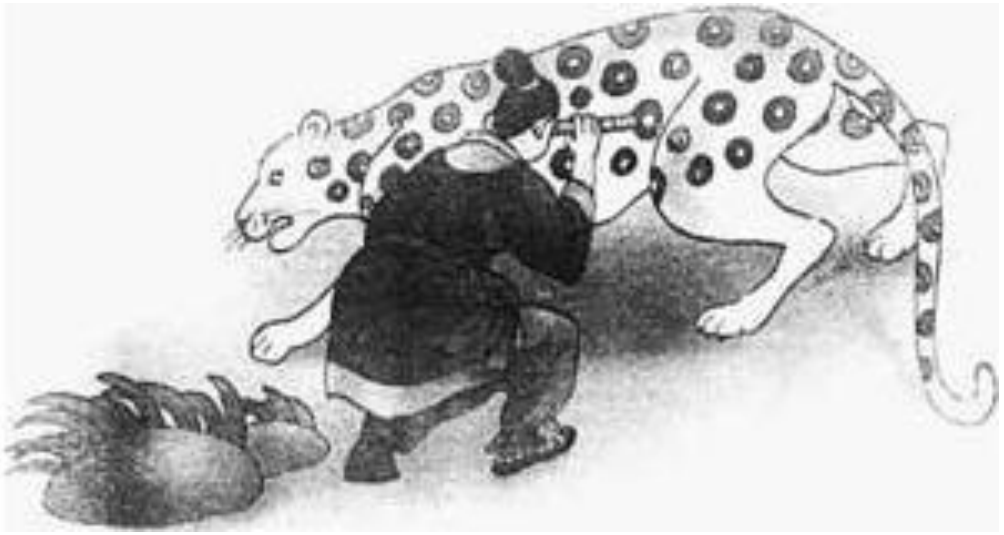
APT组织使用LIVING-OFF-THE-LAND(LOTL)技术

- 系统命令
  - net, certutil, ipconfig, bitsadmin, netsh, …
- 系统内置环境
  - Msbuild, csc, …
  - PubPrn.vbs
- 应用环境
  - IIS： appcmd.exe
- 其他
  - psexec, …

窥一斑而知全貌

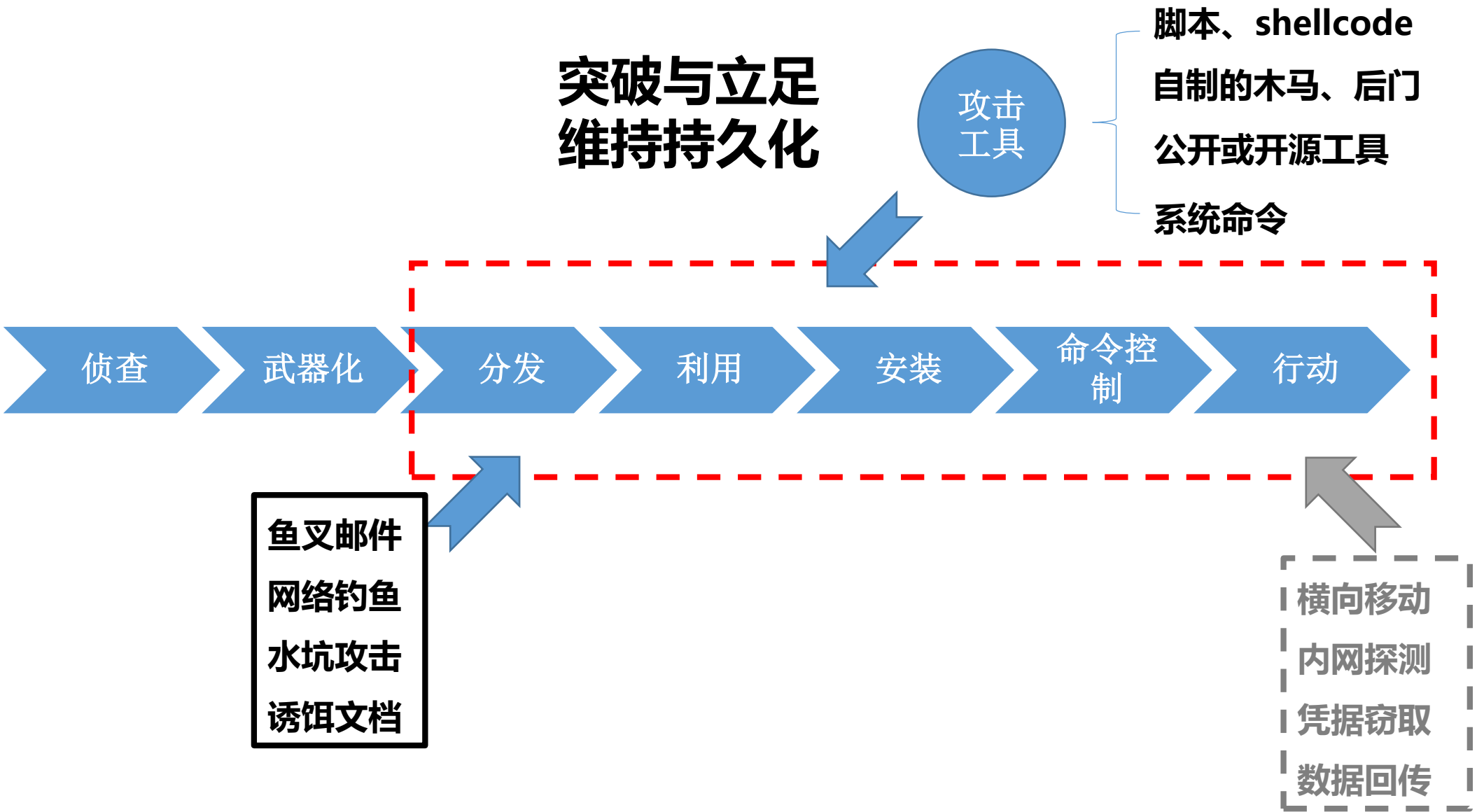
通过碎片化的证据还原攻击全貌





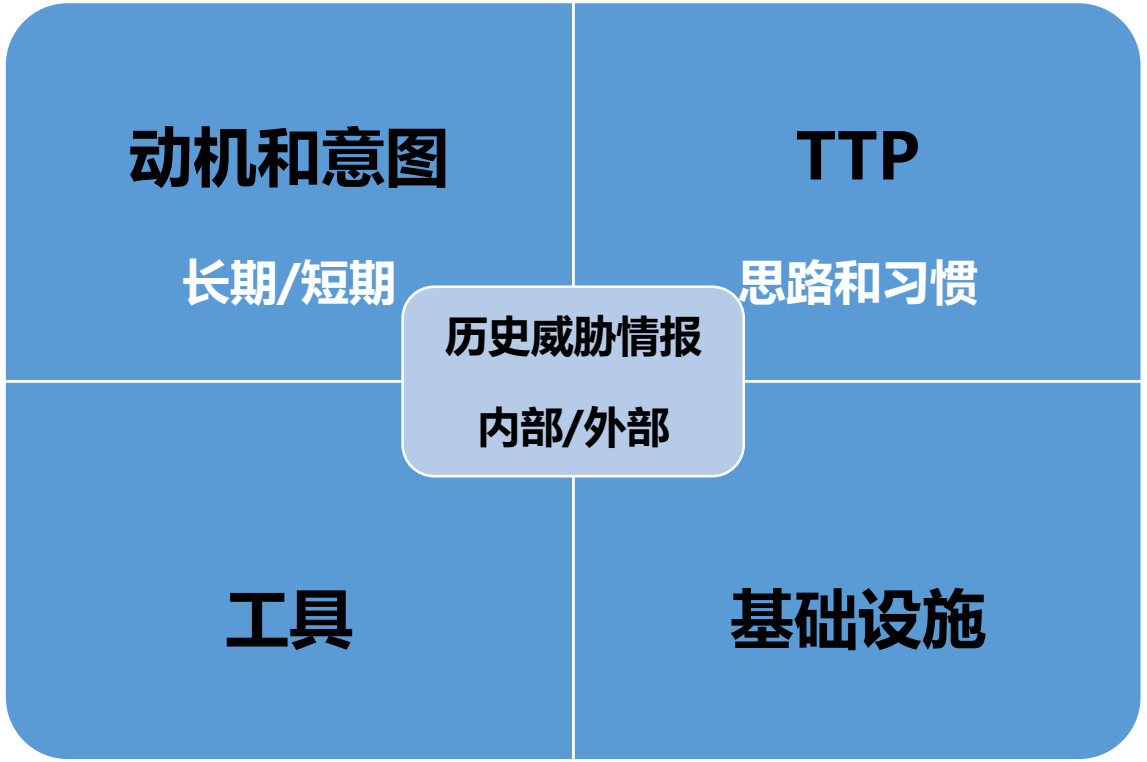
图片来源网络

分析与狩猎


突破与立足
维持持久化
攻击工具
脚本、shellcode
自制的木马、后门
公开或开源工具
系统命令
侦查
武器化
分发
利用
安装
命令控制
行动
鱼叉邮件
网络钓鱼
水坑攻击
诱饵文档
横向移动
内网探测
凭据窃取
数据回传

分析与狩猎

- 技术分析
  - 特征
- 战术分析
  - 阶段
- 意图分析
  - 目标
- 归属分析
  - 可靠性



易变的

Drive-by Compromise

ID: T1189

Tactic: Initial Access

Platform: Windows, Linux, macOS

Permissions Required: User

Data Sources: Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Version: 1.0

- 利用失陷站点作为基础设施
  - URI路径
- 修改失陷站点文件
  - 插入JS片段
  - 外链JS脚本

分析与狩猎

behavior:"powershell.exe" AND behavior:"csc.exe"

PowerShell

ID: T1086

Tactic: Execution

Platform: Windows

Permissions Required: User, Administrator

Data Sources: PowerShell logs, Loaded DLLs, DLL monitoring, Windows Registry, File monitoring, Process monitoring, Process command-line parameters

Supports Remote: Yes

Contributors: Praetorian

Version: 1.1

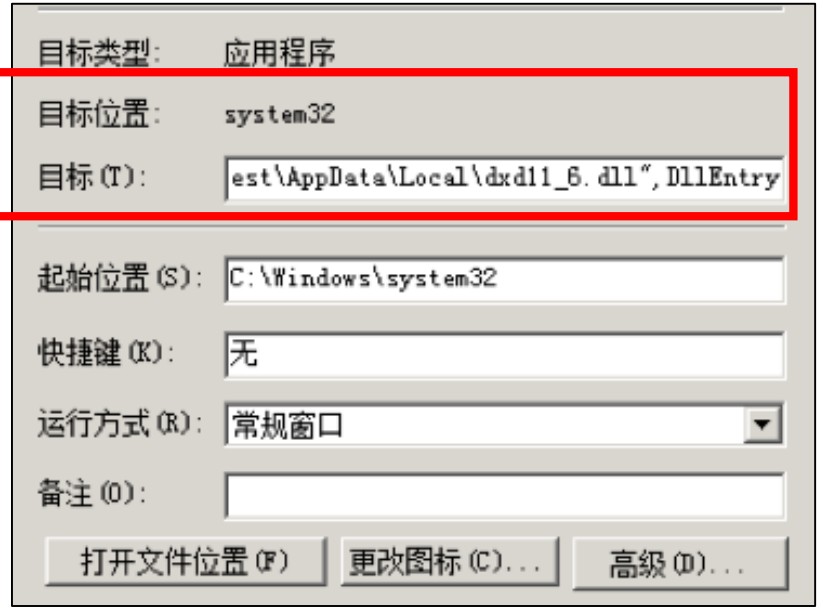
- 语法灵活
- 特殊参数
  - -exec bypass
  - -enc
  - iex

behavior:"powershell.exe" AND behavior:"csc.exe"

FILES 324

40584cbe4c043e796d8987f10fba1b515909398ce74b4d9323596678fab07675 /tmp/eml_attach_for_scan/33d54fd6143201d04d1c7684b05f161a.file rtf ole-embedded	23 / 59
0f4d294e40eb481ad192ce3670ab90120becb761e1b28a68f0c6eb439a4cf4bb name rtf ole-embedded	23 / 58
f432c6dbcae866646011b0229f79e0828e8c0a20dd5e11b32308f90353d85ab2 Qoutes 4724.doc doc macros obfuscated	14 / 61
fd4f1e6e95e361b31e2ec863b431ec327e1e45b080ffa4b6b7ad29f0a9d72001 /tmp/eml_attach_for_scan/0ced8b1472c3901de6caec8ba3b0be13.file rtf ole-embedded	22 / 58
62020cbc3aaab1af58b951d214fa16b54ec865e8d8f4ded045a380d488bd6c26 name rtf ole-embedded	22 / 57
998de7529ce2dab5805dc54b950fe8fb864da9d893aa498dd355786b63d9f9cb name rtf ole-embedded	22 / 58
30d005c68fb77006bbada70c2d8ba8013c651eef5d8d421906eeb1ca9948c05e rtf ole-embedded	22 / 58
98ec340830dcbc3535c88612fa0c40caa7a4c0ad656bf8aa232b3b35d4a7a028 bt.exe peexe	11 / 67
67e21b5002ebd96d8f5b8600a2ab8558af950abb377c256069cdf075408083a9 xls auto-open macros obfuscated	24 / 58

Shortcut Modification



域名注册：一次注册，分批使用

事件1

https://ti.qianxin.com/search?type=domain&value=philtimes.org

威胁研判分析 philtimes.org

philtimes.org

OCEANLOTUS

其他类型恶意网址

流行度

动态域名 否

隐私保护 是

白名单 否

创建时间 2017/04/28

更新时间 2017/06/28

过期时间 2018/04/28

最近看到 2019/06/04

威胁情报 1 域名解析 1 注册信息 5 关联域名 2 数字证书 50

当前注册信息

创建时间	2017-04-28 07:57:05
过期时间	2018-04-28 07:57:05
更新时间	2017-06-28 03:45:50
注册人	Domain Administrator
注册人所属组织	See PrivacyGuardian.org （ 相关域名0个 ）
管理员邮箱	pw-77041845b6c3d6b9aaaae8ac13b1a5e1@privacyguardian.org （ 相关域名0个 ）
管理员电话	+1.3478717726
管理员传真	
国家	UNITED STATES
域名服务商	
域名服务器	aria.ns.cloudflare.com , jeff.ns.cloudflare.com

事件2

https://ti.qianxin.com/search?type=domain&value=cambodiadaily.org

威胁研判分析 cambodiadaily.org

cambodiadaily.org

OCEANLOTUS

威胁情报 1 域名解析 0 注册信息 13 关联域名 4 数字证书 100

过期时间	2015-01-13 17:01:08
更新时间	2014-03-28 04:12:25

注册信息

创建时间	2017-04-28 07:42:46
过期时间	2018-04-28 07:42:46
更新时间	2017-04-28 07:50:09
注册人	Domain Administrator

事件3

https://ti.qianxin.com/search?type=domain&value=coleope.com

威胁研判分析 coleope.com

coleope.com

OCEANLOTUS

流行度

动态域名 否

威胁情报 域名解析 2 注册信息

当前注册信息

创建时间	2017-04-28
过期时间	2018-04-28
更新时间	2017-04-28

https://ti.qianxin.com/search?type=domain&value=ailloux.com

威胁研判分析 ailloux.com

ailloux.com

OCEANLOTUS

流行度

动态域名 否

威胁情报 域名解析 0 注册信息

当前注册信息

创建时间	2017-04-27
过期时间	2018-04-27
更新时间	2017-04-28

https://ti.qianxin.com/search?type=domain&value=befmann.com

威胁研判分析 befmann.com

befmann.com

OCEANLOTUS

流行度

动态域名 否

威胁情报 域名解析 2 注册信息

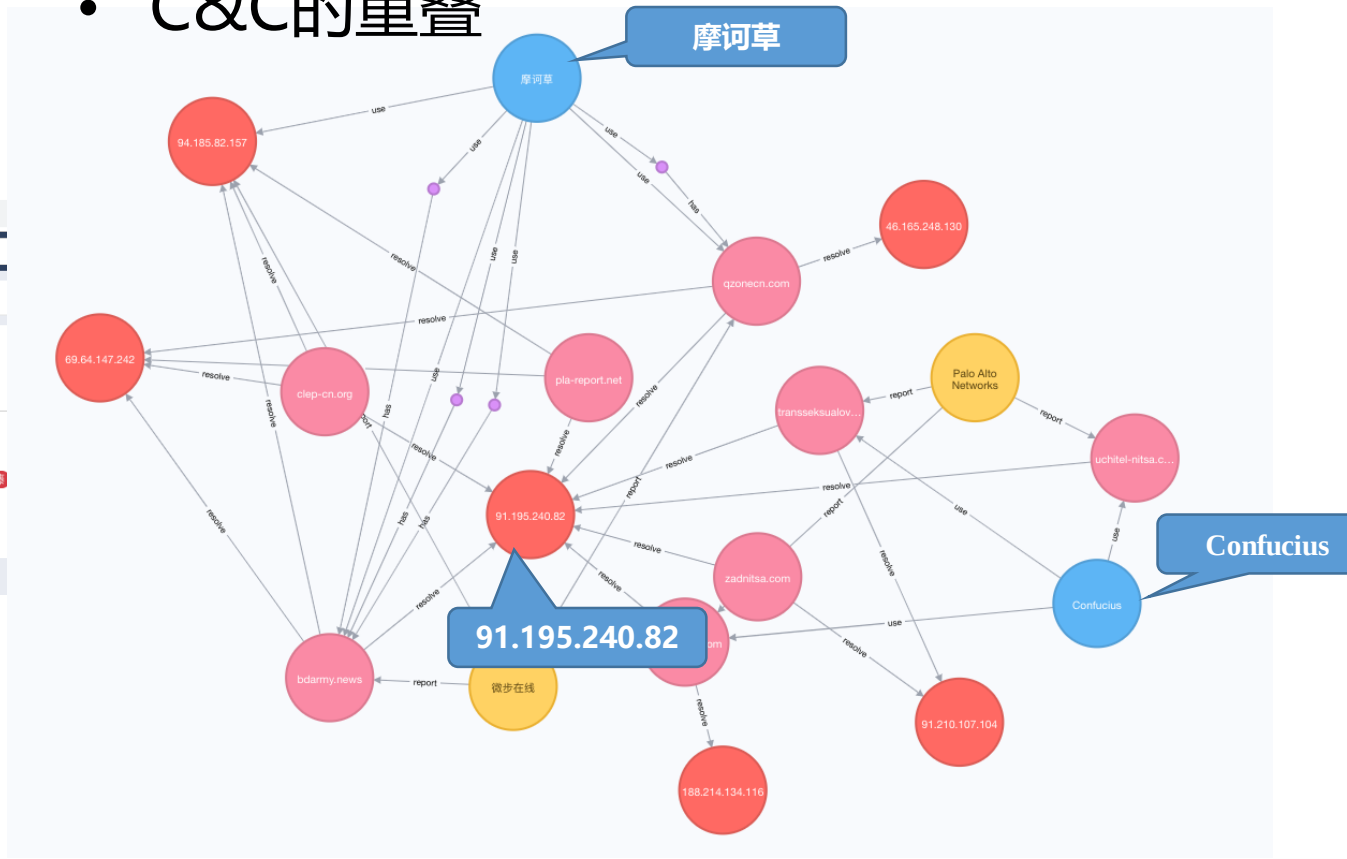
当前注册信息

创建时间	2017-04-28
过期时间	2018-04-28
更新时间	2017-04-28

分析与狩猎

DNS记录的变更

- C&C的重叠



分析与狩猎

- COBALT STRIKE TEAM SERVERS
  - 响应头部多的空格
- ANIMAL FARM
  - User-Agent MSIE -> MSI

```
00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 20   HTTP/1.1  200 OK
00000010  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ..Conten t-Type:
00000020  61 70 70 6c 69 63 61 74  69 6f 6e 2f 6f 63 74 65   applicat ion/octe
00000030  74 2d 73 74 72 65 61 6d  0d 0a 44 61 74 65 3a 20   t-stream ..Date:
00000040  46 72 69 2c 20 38 20 4a  61 6e 20 32 30 31 36 20   Fri, 8 J an 2016
00000050  31 35 3a 31 37 3a 35 30  20 47 4d 54 0d 0a 43 6f   15:17:50  GMT..Co
00000060  6e 74 65 6e 74 2d 4c 65  6e 67 74 68 3a 20 30 0d   ntent-Le ngth: 0.
00000070  0a 0d 0a                                           ...
```

https://blog.fox-it.com/2019/02/26/identifying-cobalt-strike-team-servers-in-the-wild/

User-Agent: Mozilla/4.0 (compatible; MSI 6.0; Windows NT 5.1; .NET CLR 1.0.3705; .NET CLR 1.1.4322)

- TURLA劫持APT34的控制基础设施

总结

- ATT&CK对APT威胁的分析、跟踪和狩猎提供了指导性知识基础
- 在实际的APT威胁中，ATT&CK的覆盖程度和粒度并不能完全适用，需要加以丰富
- ATT&CK是由运营IOC层面进一步到运营TTP层面

关注我们

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE