當 AI 遇到 MITRE ATT&CK：抓出惡意程式意圖，玩轉駭客 TTPs

黃意婷
臺灣科技大學 電機工程系 助理教授

黃意婷

- 臺灣大學資訊管理博士
- 現職
  - 臺灣科技大學電機工程系助理教授
  - 臺灣大學資訊管理學系兼任助理教授
- 經歷
  - 中央研究院博士後研究學者
  - 美國德州農工大學博士後研究學者
  - 美國卡內基梅隆大學訪問學者
- 近年來參與多項科技部與產學合作計畫

Outline

Malware Analysis

MITRE ATT&CK

MAMBA

MAMBA+

本週重大資安新聞

- 勒索軟體DeadBolt攻擊兩個月爆增近7倍，臺灣受害排第4
- 中國駭客鎖定亞洲政府，以舊版合法軟體元件從事間諜行動
- 北約文件流入暗網，起因是葡萄牙軍方遭網路攻擊
- 駭客鎖定PyPI套件開發者發動網釣攻擊，意圖植入竊密軟體
- 惡意軟體Bumblebee藉後滲透工具PowerSploit運作於記憶體
- 微軟公布9月例行修補，揭露63個漏洞的資訊與緩解措施
- WordPress外掛程式BackupBuddy、WPGateway存零時差漏洞
- 電腦版Teams應用程式竟以明文儲存用戶身分驗證資料
- 旅遊業者KKday前經理涉竊密供新東家運用，遭檢調約談
- 爲規避偵測，駭客近年改以間歇式手法加密受害電腦檔案

往下看更多 iThome編製 2022/9/17

FIREEYE™ PRODUCTS CUSTOMERS

高度規避的攻擊者利用SolarWinds供應鏈，利用SUNBURST後門對全球多個受害者進行攻擊

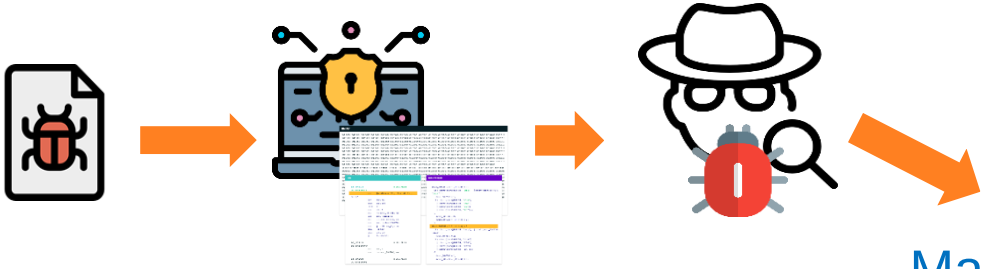
December 13, 2020 | by FireEye

執行摘要

- 我們發現了一個全球性的入侵活動，我們正在追蹤這個活動的幕後黑手是UNC2452。
- FireEye 發現了一個利用 SolarWinds Orion 商業軟體更新木馬化的供應鏈攻擊，以散佈我們稱為 SUNBURST 的惡意軟體。
- 攻擊者在入侵後的活動利用多種技術來逃避檢測並掩飾他們的活動，但這些技術也為提供了機會讓我們檢測到。
- 該活動範圍很廣，影響到世界各地的公共和私人機構。
- FireEye正在發布特徵碼，以檢測這種威脅行為者和現有流通 (in the wild) 針對供應鏈的攻擊。這些都可以在我們的公共GitHub頁面上找到。 FireEye的產品和服務可以幫助客戶檢測和阻止這種攻擊。

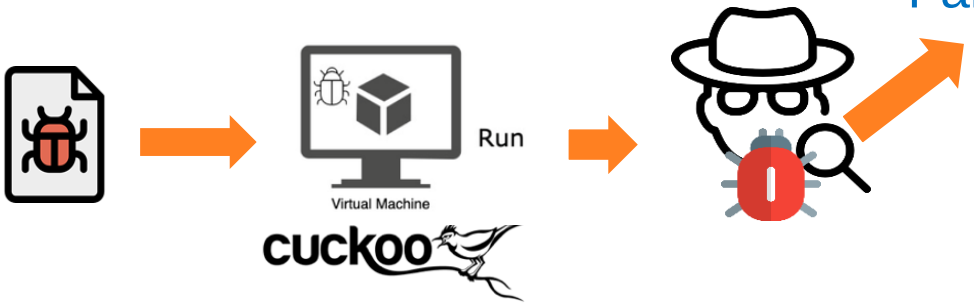
Malware Analysis

Static Analysis



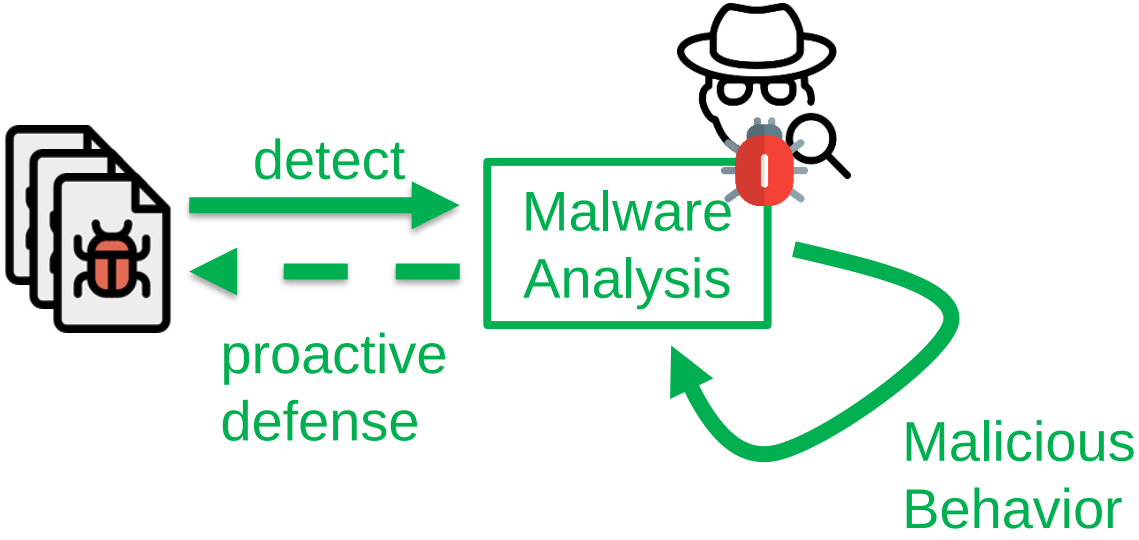
IDA Pro

Dynamic Analysis



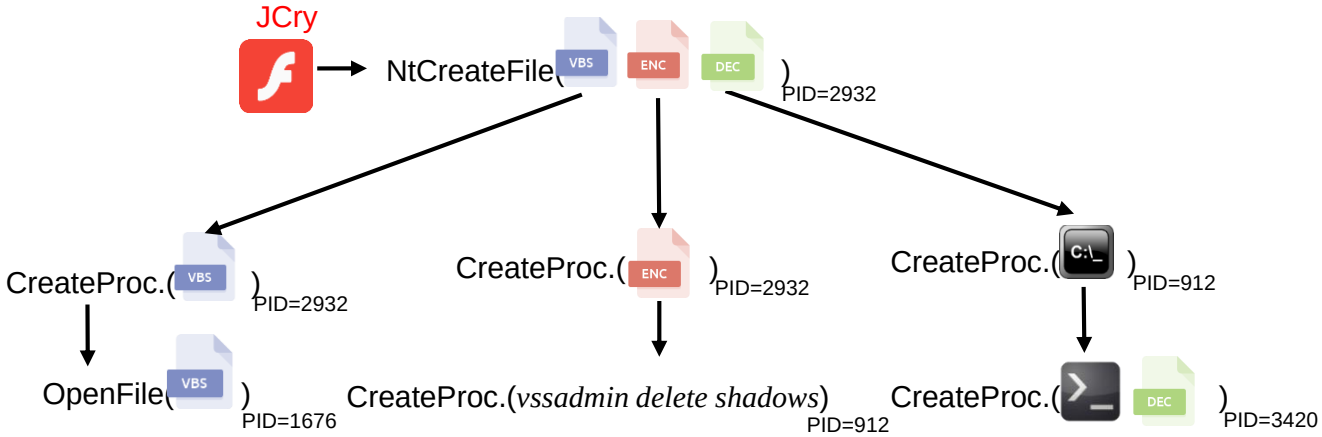
Malware Detection
Family Classification

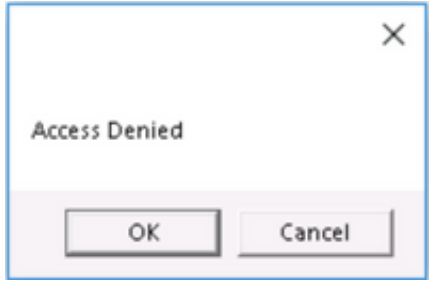
Why We Care Malicious Behavior (TTPs)?



an Adobe flash player update installer

JCry





an Adobe flash player update installer

JCry

T1547.001 Autostart Execution: Startup Folder

NtCreateFile(VBS ENC DEC) PID=2932

T1059.005 Command and Scripting Interpreter: Visual Basic

T1486 Data Encrypted for Impact

T1059.003 Command and Scripting Interpreter: Windows Command Shell

CreateProc.(VBS) PID=2932

CreateProc.(ENC) PID=2932

CreateProc.(C:_) PID=912

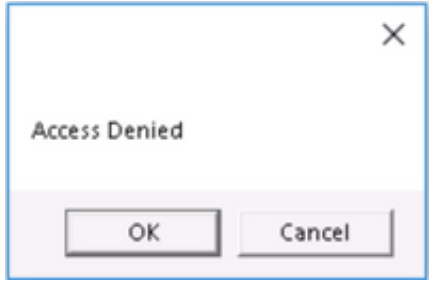
T1490 Inhibit System Recovery

T1059.001 Command and Scripting Interpreter: PowerShell

OpenFile(VBS) PID=1676

CreateProc.(*vssadmin delete shadows*) PID=912

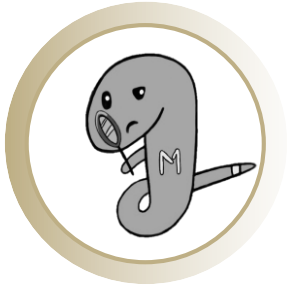
CreateProc.(DEC) PID=3420



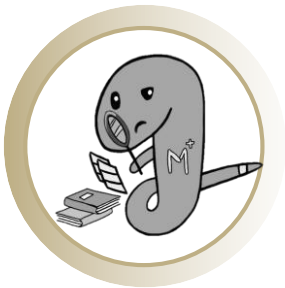
Outline

Malware Analysis

MITRE ATT&CK



MAMBA



MAMBA+

MITRE ATT&CK

Adversarial Tactics, Techniques and Common Knowledge

https://attack.mitre.org/

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Resources | Blog
Contribute | Search

MATRICES

- Enterprise
  - PRE
  - Windows
  - macOS
  - Linux
  - Cloud
  - Network
  - Containers
- Mobile
- ICS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
9 techniques	10 techniques	18 techniques	13 techniques	34 techniques	15 techniques	25 techniques
Drive-by Compromise	Command and Scripting Interpreter (5)	Account Manipulation (2)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Adversary-in-the-Middle (3)	Account Discovery (3)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (10)	Boot or Logon Autostart Execution (10)	BITS Jobs	Credentials from Password Stores (3)	Browser Bookmark Discovery
Hardware Additions	Native API	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Debugger Evasion	Exploitation for Credential Access	Debugger Evasion
Phishing (3)	Scheduled Task/Job (2)	Browser Extensions	Create or Modify System Process (1)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (2)	Direct Volume Access	Forge Web Credentials (2)	File and Directory Discovery
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (2)	Escape to Host	Domain Policy Modification (2)	Input Capture (4)	Group Policy Discovery
Trusted Relationship	System Services (1)	Create or Modify System Process (1)	Event Triggered Execution (11)	Execution Guardrails (1)	Modify Authentication Process (3)	Network Service Discovery
Valid Accounts (3)	User Execution (2)	Event Triggered Execution (11)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Network Share Discovery
	Windows Management Instrumentation	External		File and Directory Permissions Modification (1)		Network Sniffing
				Hide Artifacts (9)		Password Policy Discovery
				Hijack Execution		Peripheral Device

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Resources | Blog
Contribute | Search

MATRICES

- Enterprise
  - PRE
  - Windows
  - macOS
  - Linux
  - Cloud
  - Network
  - Containers
- Mobile
- ICS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
9 techniques	10 techniques	18 techniques	13 techniques	34 techniques	15 techniques	25 techniques
Drive-by Compromise	Command and Scripting Interpreter (5)	Account Manipulation (2)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Adversary-in-the-Middle (3)	Account Discovery (3)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (10)	Boot or Logon Autostart Execution (10)	BITS Jobs	Credentials from Password Stores (3)	Browser Bookmark Discovery
Hardware Additions	Native API	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Debugger Evasion	Exploitation for Credential Access	Debugger Evasion
Phishing (3)	Scheduled Task/Job (2)	Browser Extensions	Create or Modify System Process (1)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (2)	Direct Volume Access	Forge Web Credentials (2)	File and Directory Discovery
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (2)	Escape to Host	Domain Policy Modification (2)	Input Capture (4)	Group Policy Discovery
Trusted Relationship	System Services (1)	Create or Modify System Process (1)	Event Triggered Execution (11)	Execution Guardrails (1)	Modify Authentication Process (3)	Network Service Discovery
Valid Accounts (3)	User Execution (2)	Event Triggered Execution (11)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Network Share Discovery
	Windows Management Instrumentation	External		File and Directory Permissions Modification (1)		Network Sniffing
				Hide Artifacts (9)		Password Policy Discovery
				Hijack Execution		Peripheral Device

The new v11.2 release of MITRE ATT&CK contains a beta version of Sub-Techniques for Mobile. The current, stable Mobile content can be accessed via the v10 release URL.

TECHNIQUES

Registry Run Keys / Startup Folder
Authentication Package
Time Providers
Winlogon Helper DLL
Security Support Provider
Kernel Modules and Extensions
Re-opened Applications
LSASS Driver
Shortcut Modification
Port Monitors
Print Processors
XDG Autostart Entries
Active Setup
Login Items
Boot or Logon Initialization Scripts

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Other sub-techniques of Boot or Logon Autostart Execution (14)

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.[1] These programs will be executed under the context of the user and will have the account's associated permissions level.

Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is `C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`. The startup folder path for all users is `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp`.

The following run keys are created by default on Windows systems:

ID: T1547.001
Sub-technique of: T1547
Tactics: Persistence, Privilege Escalation
Platforms: Windows
Permissions Required: Administrator, User
CAPEC ID: CAPEC-270
Contributors: Oddvar Moe, @oddvarmoe
Version: 1.1
Created: 23 January 2020
Last Modified: 12 May 2022

Version Permalink

Source: T1547.001

TECHNIQUES

- Registry Run Keys / Startup Folder
- Authentication Package
- Time Providers
- Winlogon Helper DLL
- Security Support Provider
- Kernel Modules and Extensions
- Re-opened Applications
- LSASS Driver
- Shortcut Modification
- Port Monitors
- Print Processors
- XDG Autostart Entries
- Active Setup
- Login Items
- Boot or Logon Initialization

Procedure Examples

ID	Name	Description
S0045	ADVSTORESHELL	ADVSTORESHELL achieves persistence by adding itself to the `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` Registry key.[5][6][7]
S0331	Agent Tesla	Agent Tesla can add itself to the Registry as a startup program to establish persistence.[8][9]
S0622	AppleSeed	AppleSeed has the ability to create the Registry key name `EstsoftAutoUpdate` at `HKLU\Software\Microsoft/Windows\CurrentVersion\RunOnce` to establish persistence.[10]
G0026	APT18	APT18 establishes persistence via the `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` key.[11][12]
G0073	APT19	An APT19 HTTP malware variant establishes persistence by setting the Registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows Debug Tools-%LOCALAPPDATA%\`.[13]
G0007	APT28	APT28 has deployed malware that has copied itself to the startup directory for persistence.[14]
G0016	APT29	APT29 added Registry Run keys to establish persistence.[15]
G0022	APT3	APT3 places scripts in the startup folder for persistence.[16]

Source: T1547.001

Outline

Malware Analysis

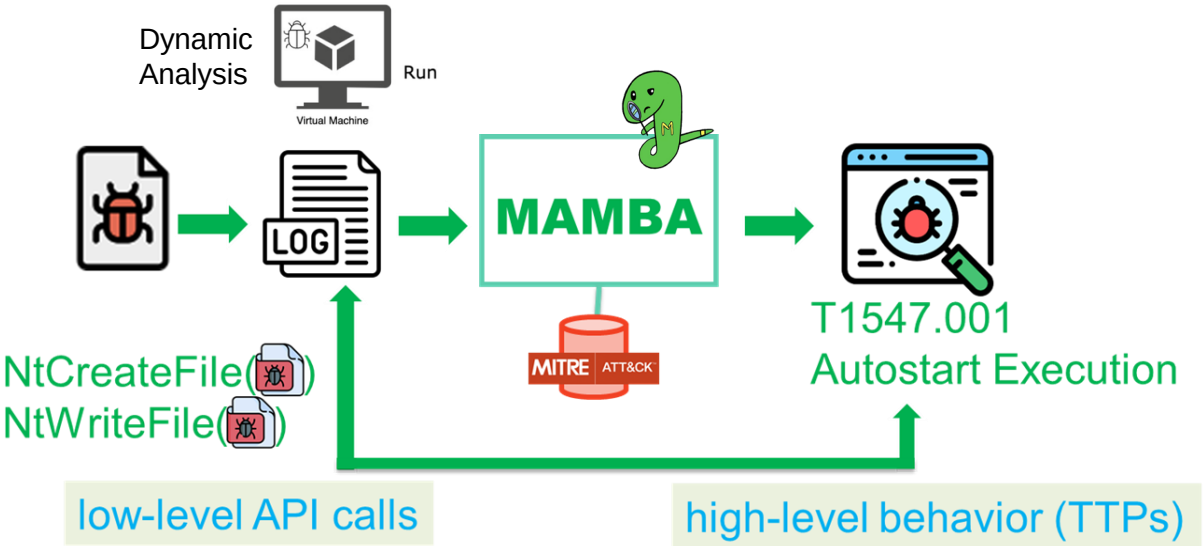
MITRE ATT&CK

MAMBA

MAMBA+

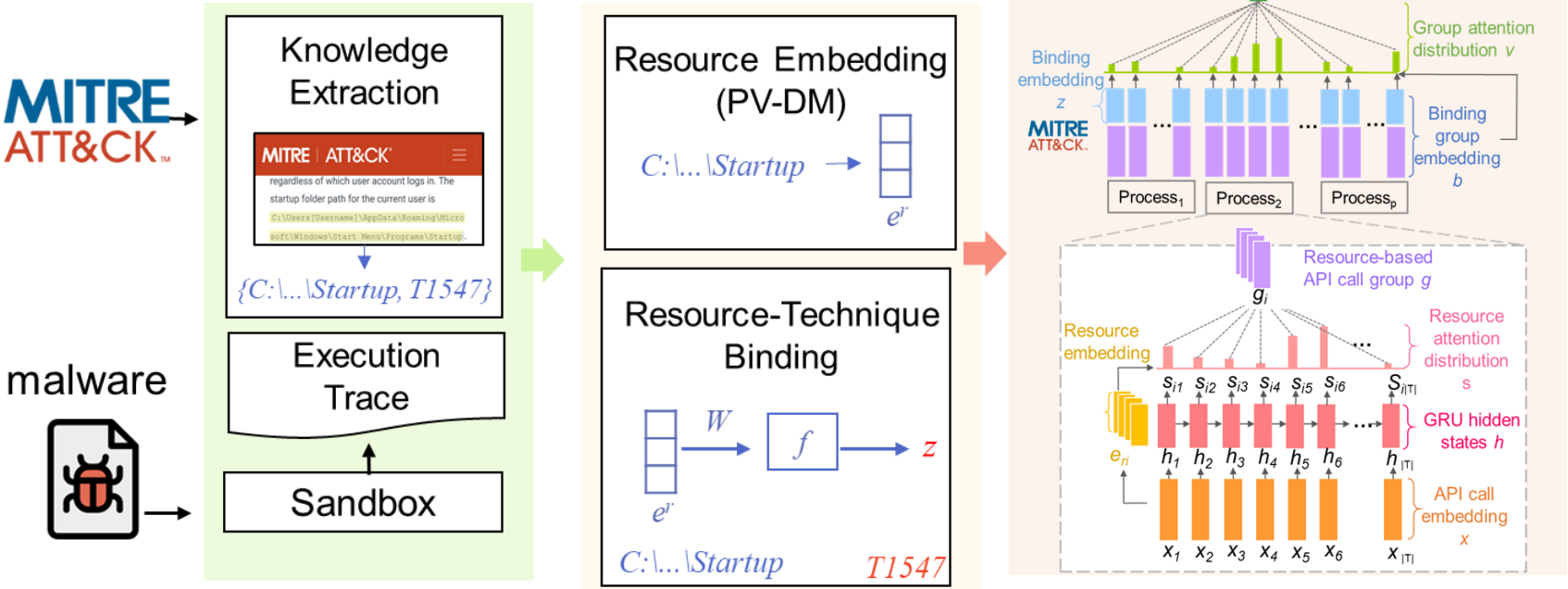
MAMBA

Malware Analysis with MITRE ATT&CK

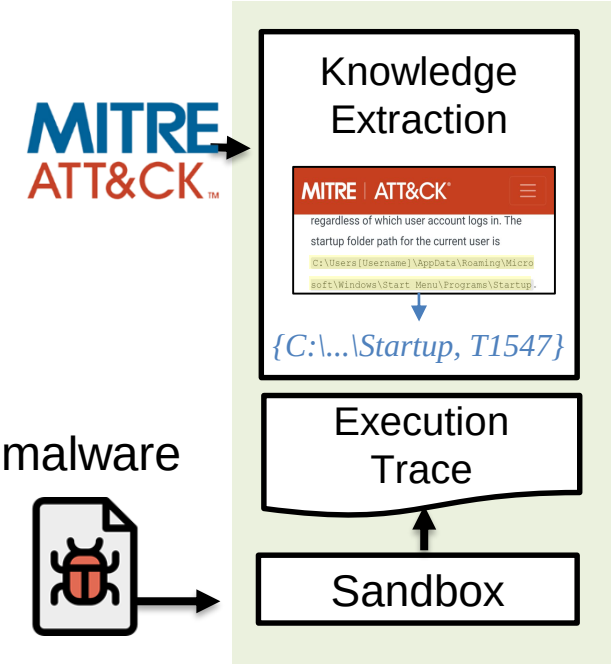


Icons made by Freepik from www.flaticon.com

MAMBA



Extraction | Fusion | Threat Identification



Extraction

MITRE | ATT&CK®

regardless of which user account logs in. The startup folder path for the current user is `C:\Users[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`.

```
"category": "file",
"api": "NtCreateFile",
"arguments": {
    "filepath":
    "C:\\Users\\Baka\\AppData\\Roaming
    \\Microsoft\\Windows\\Start
    Menu\\Programs\\Startup\\Enc.exe
},


"category": "file",
"api": "NtWriteFile",
"arguments": {
    "filepath":
    "C:\\Users\\Baka\\AppData\\Roaming
    \\Microsoft\\Windows\\Start
    Menu\\Programs\\Startup\\Enc.exe"
```

cuckoo

How accurate **MAMBA** is?

- **MAMBA** achieves state-of-the-art results
  - F1 59% in ATT&CK dataset
  - F1 95%, 89% in Big dataset (ATT&CK + MalShare)

	Source	ATT&CK dataset					Big dataset (ATT&CK + MalShare)									
	Label	ATT&CK					Cuckoo					RegExp				
	Metric	P	R	F1	FPR	FNR	P	R	F1	FPR	FNR	P	R	F1	FPR	FNR
Rule-based	Cuckoo	0.078⋆	0.048⋆	0.049⋆	0.044⋆	0.858⋆	-					0.087⋆	0.326⋆	0.131⋆	0.036⋆	0.903⋆
	RegExp	0.081⋆	0.206⋆	0.099⋆	0.351⋆	0.659⋆	0.061⋆	0.231⋆	0.092⋆	0.283⋆	0.468⋆	-				
ML-based	Random Forest	0.375†	0.144⋆	0.208⋆	0.005⋆	0.429⋆	0.417⋆	0.203⋆	0.273⋆	0.003†	0.400	0.813⋆	0.850⋆	0.831⋆	0.010⋆	0.094⋆
	LinearSVC	0.200⋆	0.370‡	0.260⋆	0.088⋆	0.343⋆	0.380⋆	0.408⋆	0.394⋆	0.039⋆	0.298⋆	0.734⋆	0.584⋆	0.650⋆	0.046⋆	0.133⋆
	GaussianNB	0.321⋆	0.490	0.388⋆	0.092⋆	0.268†	0.349⋆	0.560⋆	0.430⋆	0.089⋆	0.217⋆	0.738⋆	0.658⋆	0.606⋆	0.047⋆	0.132⋆
	Decision Tree	0.342⋆	0.332⋆	0.337⋆	0.040⋆	0.344⋆	0.437⋆	0.464⋆	0.450⋆	0.044⋆	0.316⋆	0.745⋆	0.745⋆	0.745⋆	0.026⋆	0.113⋆
	KNeighbors	0.416⋆	0.365⋆	0.389⋆	0.028⋆	0.375⋆	0.468⋆	0.456⋆	0.462⋆	0.029⋆	0.281⋆	0.777⋆	0.772⋆	0.774⋆	0.020⋆	0.110⋆
DL-based	MLP	0.556⋆	0.365⋆	0.427⋆	0.010	0.319⋆	0.833⋆	0.779⋆	0.801⋆	0.006	0.111⋆	0.938⋆	0.926⋆	0.928⋆	0.004⋆	0.037⋆
	RNN	0.461⋆	0.214⋆	0.288⋆	0.009	0.394⋆	0.688⋆	0.604⋆	0.631⋆	0.010⋆	0.251⋆	0.850⋆	0.774⋆	0.796⋆	0.009⋆	0.115⋆
	LSTM	0.552‡	0.289†	0.362‡	0.006†	0.358⋆	0.770⋆	0.711⋆	0.735⋆	0.007	0.144⋆	0.920⋆	0.900⋆	0.908⋆	0.006⋆	0.051⋆
	MAMBA	0.667	0.569	0.591	0.011	0.220	0.898	0.887	0.891	0.006	0.061	0.945	0.954	0.949	0.005	0.024

† $p < 0.05$, ‡ $p < 0.01$, ⋆ $p < 0.001$. Mann–Whitney U test is applied to compare the performance of MAMBA against that of each compared

What **MAMBA** can do?

WannaCry (2017)

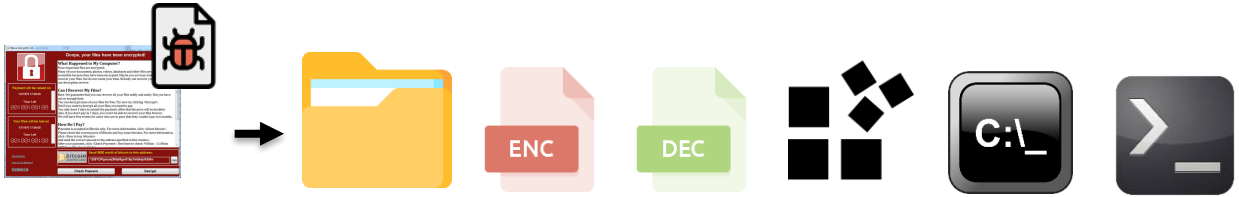
What MAMBA can do?

1. Which techniques are implemented?

Persistence/ Privilege Escalation	Execution	Defense Evasion	Discovery	Impact	Lateral Movement
T1543.003 Create Windows Service (mssecsvc2.0)	T1564.001 Hidden Files	T1222.001 File Permission Modification	T1083 File Discovery	T1490 Inhibit System Recovery	T1563.002 Remote Desktop Protocol Hijacking
	T1047 WMI: Delete Windows Shadow Copies				

What **MAMBA** can do?

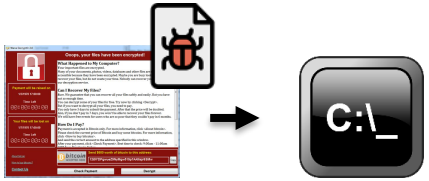
2. **Which system resources** are manipulated?



WannaCry

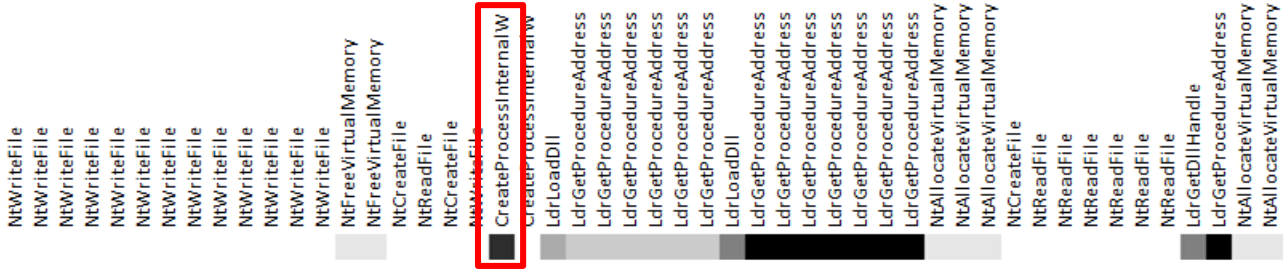
What **MAMBA** can do?

3. **What** did malware do via system resources?



T1564.001 Hidden Files
T1222.001 File Permissions Modification

WannaCry CreatePro.(attrib +h)



CreateProcessInternalW

What **MAMBA** can do?

3. **What** did malware do via system resources?

WannaCry

T1490 Inhibit System Recovery

CreatePro.(cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet)

LdrGetProcedureAddress
LdrGetProcedureAddress
CreateProcessInternalW
NtTerminateProcess
CreateDirectoryW
LdrGetDllHandle
LdrGetDllHandle
CreateDirectoryW
LdrLoadDll
LdrGetProcedureAddress
NtUnmapViewOfSection
NtUnmapViewOfSection
NtUnmapViewOfSection
LdrGetDllHandle
LdrGetProcedureAddress
NtUnmapViewOfSection
LdrGetDllHandle
LdrGetProcedureAddress
NtUnmapViewOfSection
NtFreeVirtualMemory
LdrGetDllHandle
LdrGetProcedureAddress
LdrGetDllHandle
LdrGetProcedureAddress
NtUnmapViewOfSection
NtFreeVirtualMemory
LdrGetDllHandle
NtOpenKeyEx
NtQueryValueKey
NtTerminateProcess
PAD
PAD
PAD

MAMBA

Welcome to MAMBA!

MITRE ATTACK Based Maliciousbehavior Analysis

選擇檔案 未選擇任何檔案 Submit

SolarWinds.Orion.Core.BusinessLayer.dll

Sunburst

MAMBA

Name: SunBurst
Sha256: 6b1c2706bb1b9659dfc1649f8aaf08b170880c56d50f73a4a7b969a415ee260f
Size: 645 KB
Submission date: 2021/03/27

Detected TTPs Matrix | Detected TTPs Info | Inference Softwares

Cardinal RAT	RTM	KONNI	InvisiMole
100%	100%	100%	100%
trojan	unknown	unknown	backdoor, spyware
malware type	malware type	malware type	malware type

MAMBA

Name: SunBurst
Sha256: 6b1c2706bb1b9659dfc1649f8aaf08b170880c56d50f73a4a7b969a415ee260f
Size: 645 KB
Submission date: 2021/03/27

Detected TTPs Matrix | Detected TTPs Info | Inference Softwares

- T1033
- T1056.001
- T1057
- T1059.003
- T1082
- T1112
- T1547.001

T1082 System Information Discovery

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as Systeminfo can be used to gather detailed system information. A breakdown of system data can also be gathered through the macOS systemsetup command, but it requires administrative privileges. Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine. [1] [2] [3]

MAMBA 應用範圍

➢惡意程式鑑識

作為惡意程式分析工具，提供惡意行為的高階語意與低階執行碼。

Persistence/ Privilege Escalation	Execution	Defense Evasion	Discovery	Impact	Lateral Movement
T1543.003 Create Windows Service (mssecsvc2.0)	T1564.001 Hidden Files	T1222.001 File Permission Modification	T1083 File Discovery	T1490 Inhibit System Recovery	T1563.002 Remote Desktop Protocol Hijacking
	T1047 WMI: Delete Windows Shadow Copies				

➢軟體安全查核

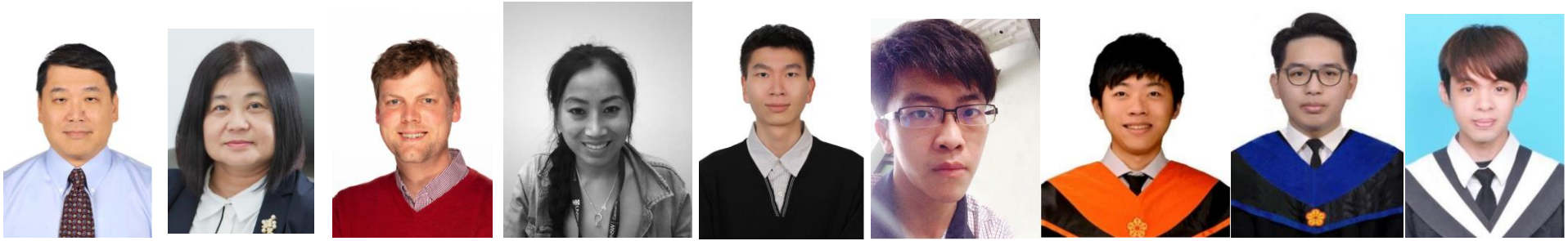
作為下載軟體檢測工具，檢驗是否被植入可疑的惡意行為。

SolarWinds.Orion.Core
.BusinessLayer.dll

Benign? or Malicious?

Icons made by SBTS2018 from www.flaticon.com

Our Team



https://www.mambaplus.tw

Icons made from www.flaticon.com