Applying MITRE to malware sandbox systems

EU ATT & CK Community

Marc Rivero López – McAfee ATR Team

McAfee

Marc Rivero López
Threat Researcher - McAfee ATR Team

Focused on:

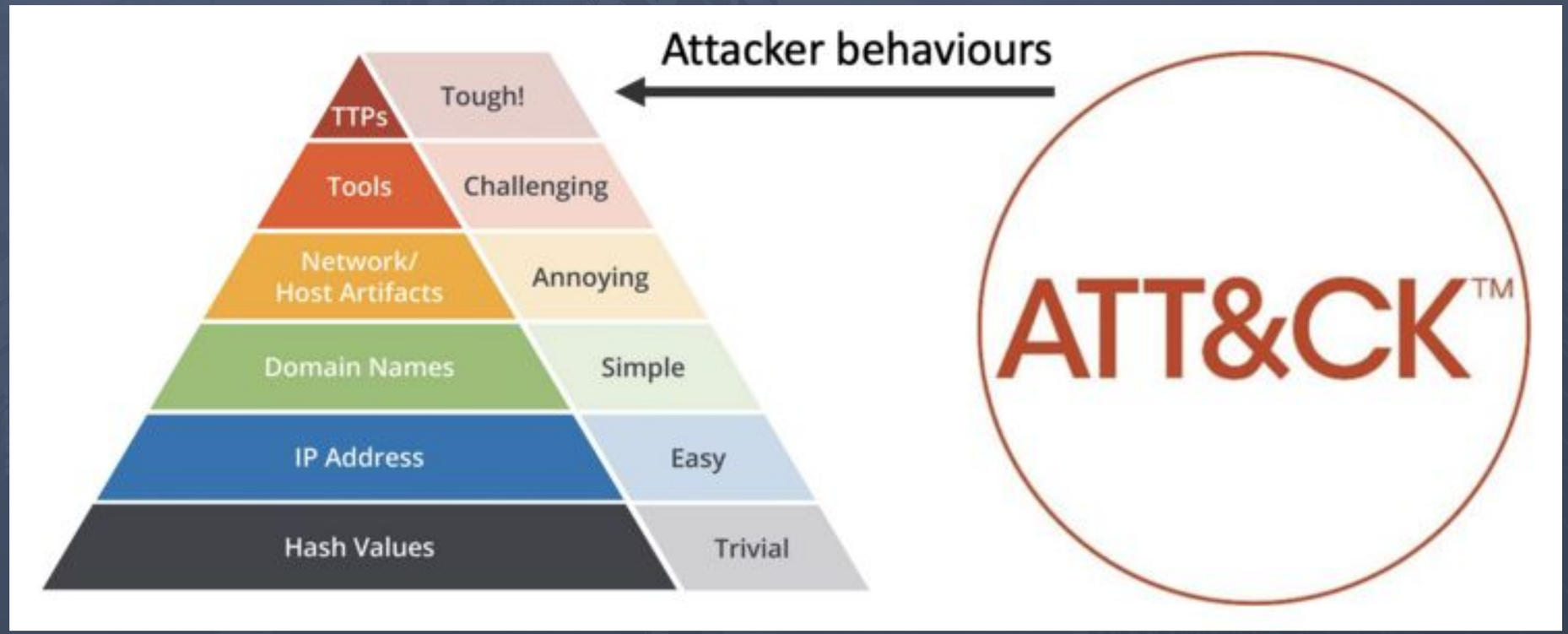
Threat Intelligence
Malware analysis

@seifreed

Why you need the MITRE ATT & CK Framework?

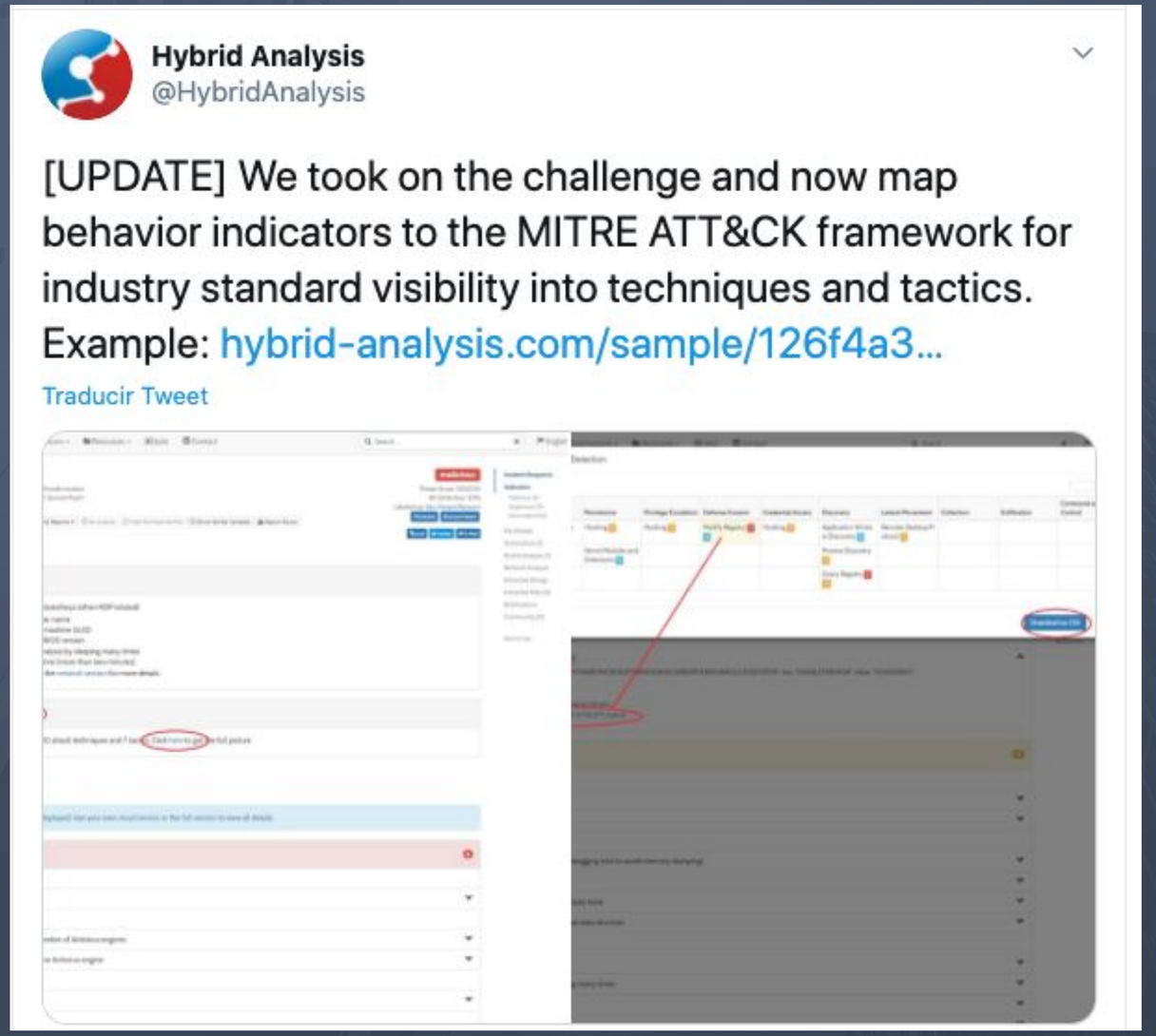
- Expand the knowledge of the network defenders and assists in prioritizing network defense by detailing the tactics, techniques, and procedures (TTPs) cyberthreats used to gain access
- Correlate specific adversaries and the techniques they have used by providing a library that details adversary groups and the campaigns they have conducted
- Gain an understanding of the specific techniques used by adversaries for named campaigns so you can evaluate and strengthen your security architecture and strategy
- Upgrade skills of junior analysts through training, which is one important step enterprises have taken to address the global cybersecurity skills shortage. The ATT&CK framework has been incorporated into many security certification courses offered by the SANS Institute and other organizations to help junior analysts better understand adversary tactics, techniques, and processes (TTPs) and apply that knowledge to improve the efficacy of their threat hunting processes.

ATT & CK and the Pyramid of Pain

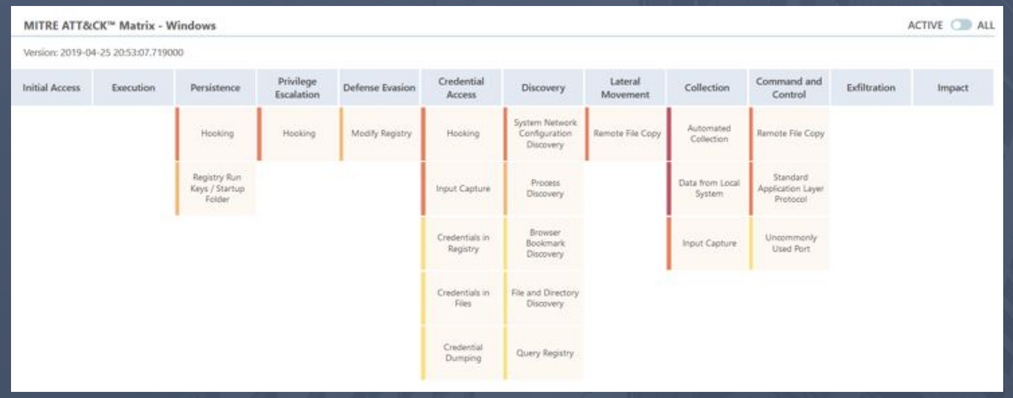


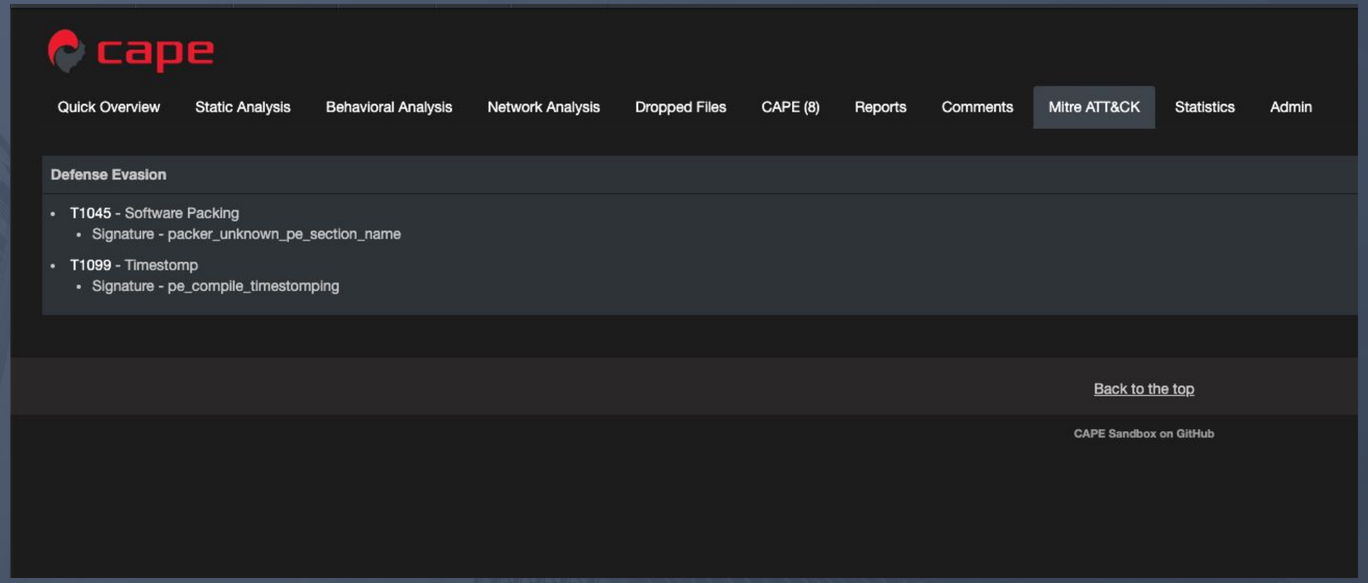
https://www.mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack

All the great histories starts someday…



MITRE integrated in sandbox systems

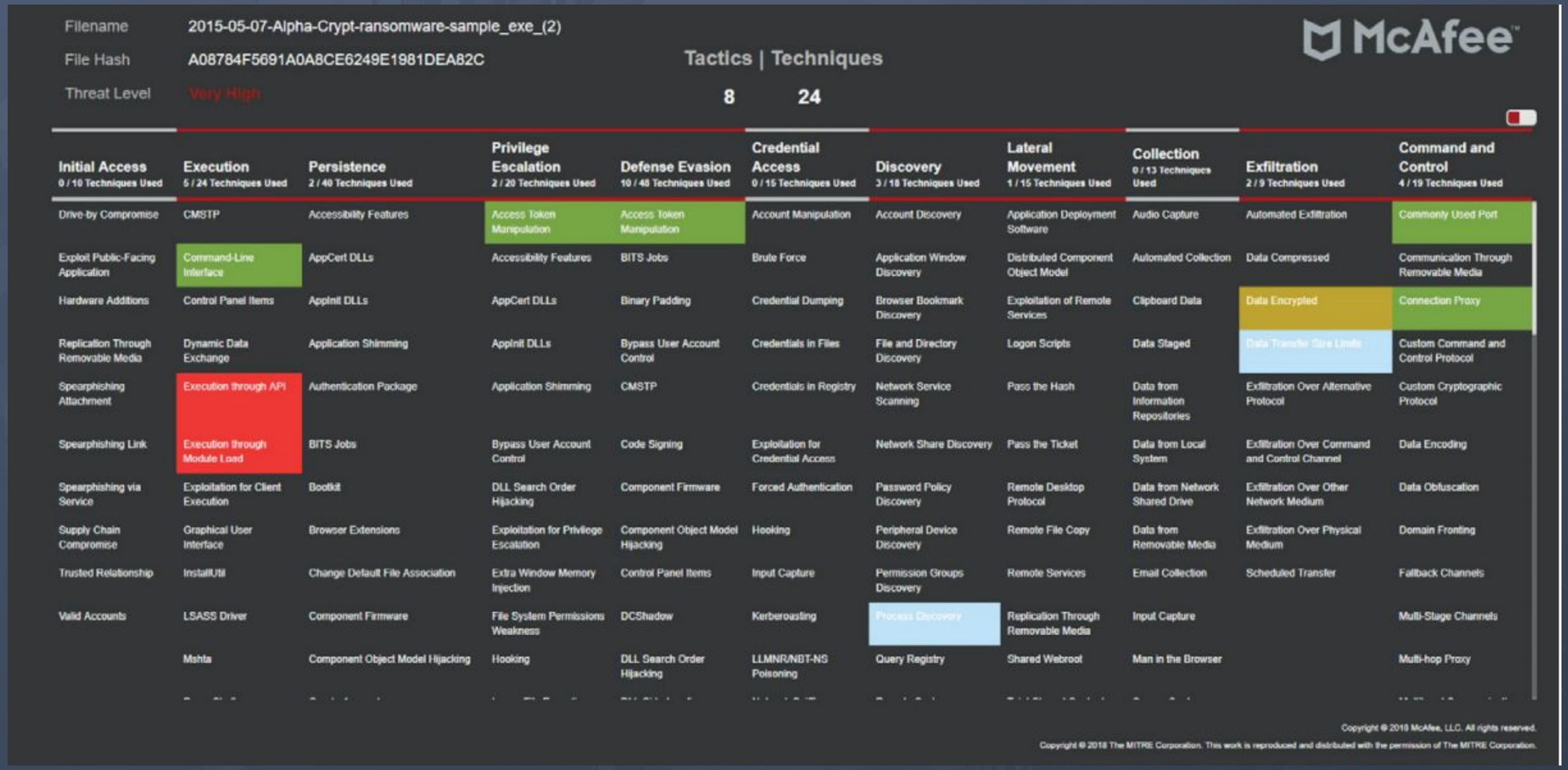




Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation 1 2 1	Winlogon Helper DLL	Access Token Manipulation 1	Masquerading 1	Credential Dumping 2	Virtualization/Sandbox Evasion 1 3	Application Deployment Software	Email Collection 1	Data Encrypted 1	Standard Cryptographic Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Replication Through Removable Media	Service Execution	Port Monitors	Process Injection 2 2	Software Packing 1 3	Credentials in Registry 1	Process Discovery 2	Remote Services	Data from Local System 2	Exfiltration Over Other Network Medium	Fallback Channels	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Disabling Security Tools 1	Input Capture	Security Software Discovery 2 2 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptographic Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Virtualization/Sandbox Evasion 1 3	Credentials in Files	File and Directory Discovery 1	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Card Swap		Premium SMS Toll Fraud
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Access Token Manipulation 1	Account Manipulation	System Information Discovery 1 1 4	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	Timestomp 1	Brute Force	System Owner/User Discovery	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port	Jamming or Denial of Service		Abuse Accessibility Features
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	Process Injection 2 2	Two-Factor Authentication Interception	Network Sniffing	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Spearphishing via Service	Third-party Software	Logon Scripts	Process Injection	Obfuscated Files or Information 2	Bash History	Network Service Scanning	Remote Desktop Protocol	Clipboard Data	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

McAfee Sandbox & MITRE techniques



Filename	2015-05-07-Alpha-Crypt-ransomware-sample_exe_(2)
File Hash	A08784F5691A0A8CE6249E1981DEA82C
Threat Level	Very High

Tactics | Techniques

8 24

Initial Access 0 / 10 Techniques Used	Execution 5 / 24 Techniques Used	Persistence 2 / 40 Techniques Used	Privilege Escalation 2 / 20 Techniques Used	Defense Evasion 10 / 48 Techniques Used	Credential Access 0 / 15 Techniques Used	Discovery 3 / 18 Techniques Used	Lateral Movement 1 / 15 Techniques Used	Collection 0 / 13 Techniques Used	Exfiltration 2 / 9 Techniques Used	Command and Control 4 / 19 Techniques Used
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy

Malware behavior map to MITRE techniques

Tales From the Trenches; a Lockbit Ransomware Story

Blog Home Categories Authors Subscribe Search Blogs

Home / Other Blogs / McAfee Labs / Tales From the Trenches a Lockbit Ransomware Story

By Marc Rivero Lopez, John Fokker and Alexandre Mundo on Apr 30, 2020

In collaboration with Northwave

As we highlighted previously across two blogs, targeted ransomware attacks have increased massively over the past months. In our first

MITRE TAXONOMY

Technique ID	Technique Description
T1107	File Deletion
T1055	Process Injection
T1112	Modify Registry
T1215	Kernel Modules and Extensions
T1060	Registry Run Keys / Start Folder
T1179	Hooking
T1055	Process Injection
T1179	Hooking
T1124	System Time Discovery
T1046	Network Service Scanning
T1083	File and Directory Discovery
T1016	System Network Configuration Discovery
T1012	Query Registry
T1082	System Information Discovery
T1057	Process Discovery
T1063	Security Software Discovery
T1047	Windows Management Instrumentation
T1035	Service Execution
T1075	Pass the Hash

The day to day of a Threat Researcher

New malware family *to research*

BazarBackdoor: TrickBot gang's new stealthy network-hacking malware

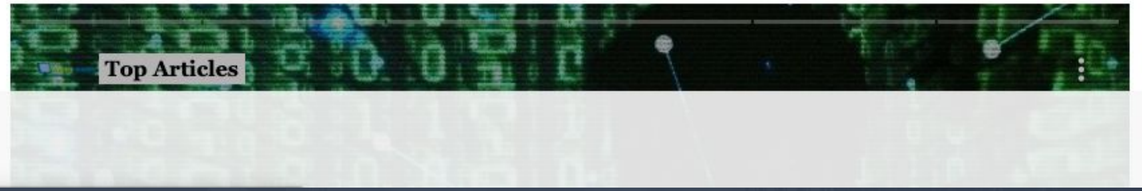
By Lawrence Abrams

April 24, 2020 01:14 PM 2

A new phishing campaign is delivering a new stealthy backdoor from the developers of TrickBot that is used to compromise and gain full access to corporate networks.

In advanced network attacks such as enterprise-targeting ransomware, corporate espionage, or data exfiltration attacks, quietly gaining access to and control over a corporate network is a mandatory step.

In new phishing attacks discovered over the past two weeks, a new malware named 'BazarBackdoor', or internally by the malware developers as simply "backdoor", is being installed that deploys a network-compromising toolkit for the threat actors.



How this threat affect *my customers?*

How can I *improve my detection* capabilities?

How can I improve *my internal products?*

Analyzing one single case

Triage phase

Public Sources

Internal data

Threat Researcher

Analysis phase

Static analysis

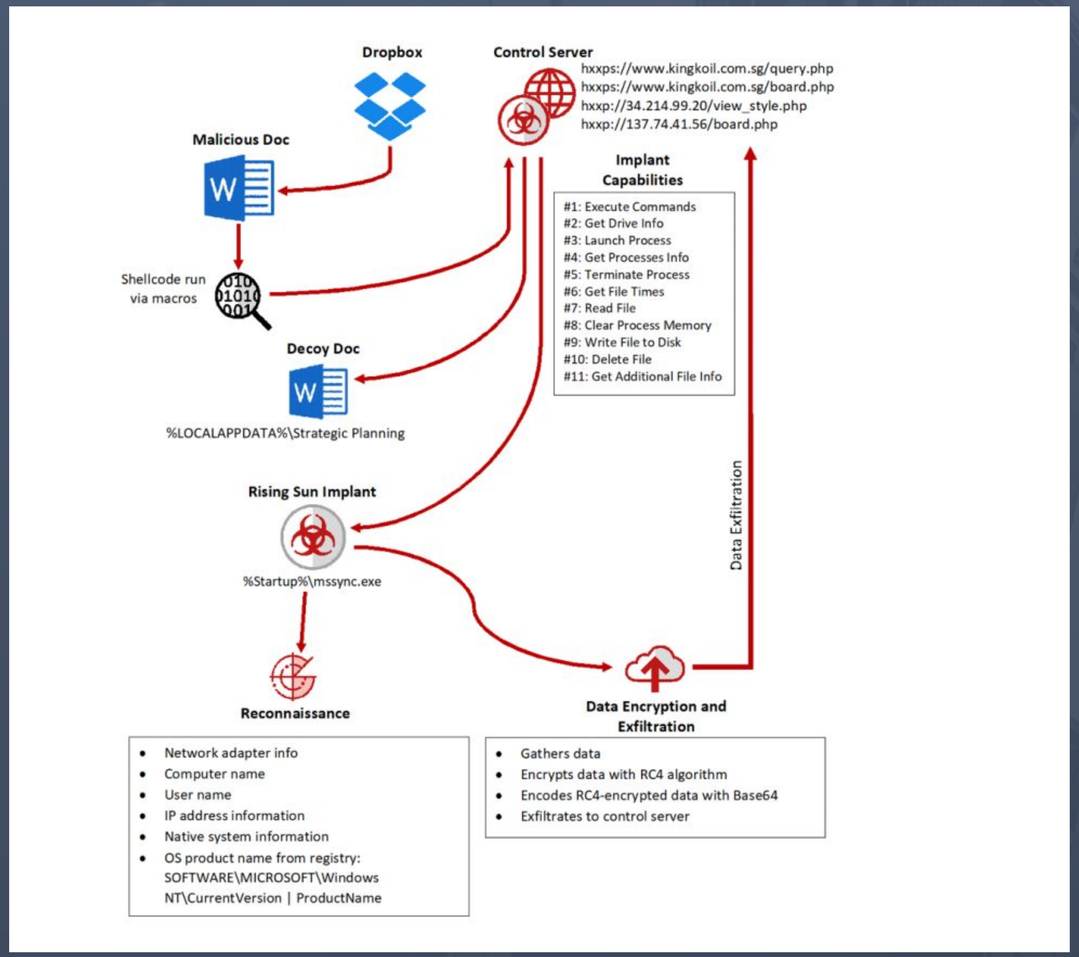
Dynamic analysis

MITRE ATT&CK™

Trickbot	techniques
Account Discovery	Files and directory discovery
Commonly used port	Hooking
Credentials in Web Browsers	Man in the browser
Credentials in files	Modify registry
Credentials in Registry	Obfuscated files or irnformation
Custom cryptographic protocol	Process injection
Data from local system	Registry Run Keys
Deobfuscate/Decode files o rinformation	Remote file copy
Disabling Security tools	Scheduled task
Domain trust discovery	Scripting
Email collection	Executable Code Obfuscation

Hunting for an unknown hash in our dataset of detonations

Finding “unknown” threats, based on malware behavior



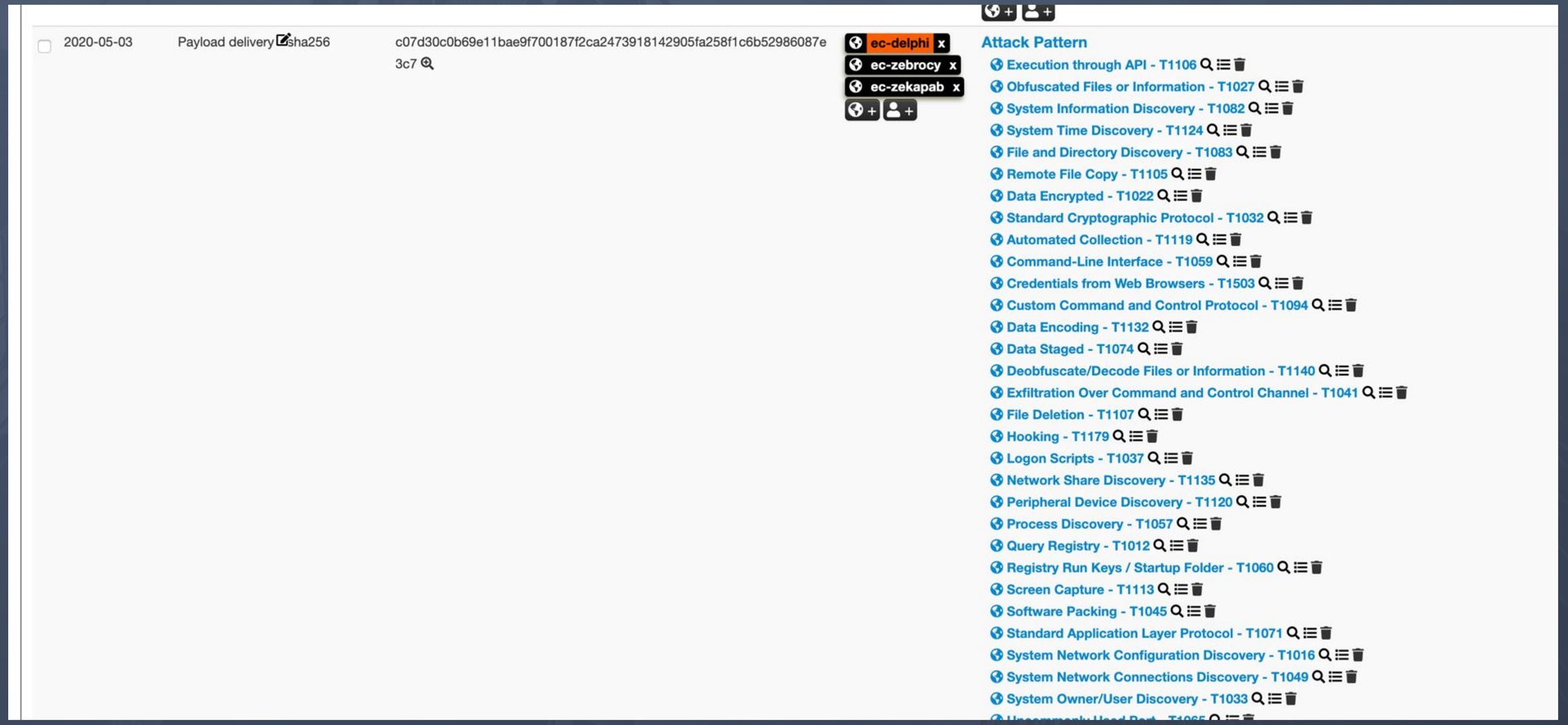
Threat Researcher

MITRE ATT&CK™

Dynamic analysis

Static analysis

An example mapping MITRE for each attribute



Malware Behavior Catalog

Malware Behavior Catalog

The Malware Behavior Catalog (MBC) is a catalog of malware objectives and behaviors, created to support malware analysis-oriented use cases, such as labeling, similarity analysis, and standardized reporting. Please see the FAQ page for answers to common questions.

Check out the MBC presentation given at BSides DC (October 2019).

To join the **MBC mailing list**, please send a request to mbc@mitre.org.

Objectives

As shown below, malware objectives are based on ATT&CK Tactics, and are tailored for the malware analysis use case of characterizing malware based on known objectives and behaviors. Two malware analysis-specific objectives not in ATT&CK are also defined (ANTI-BEHAVIORAL ANALYSIS and ANTI-STATIC ANALYSIS).

Behaviors

Under each objective, MBC captures all behaviors and code characteristics discovered during malware analysis, with links to ATT&CK Techniques as appropriate. Names of MBC behaviors may or may not match related ATT&CK techniques. Any content provided on behavior pages is *supplemental* to ATT&CK content. In other words, ATT&CK content is not duplicated in MBC, and MBC users will want to reference ATT&CK while capturing malware behaviors.

Identifiers

The first letter of a behavior identifier indicates whether the behavior is a stub referencing an ATT&CK technique ("T", matching the ATT&CK identifier; e.g. T1234), whether it enhances an ATT&CK technique with malware-specific details ("E"; e.g. E1234), or whether it is a newly defined behavior in MBC ("M"; e.g. M1234). When two or more MBC behaviors refine the same ATT&CK technique, each is given an MBC identifier and each references the ATT&CK identifier. When a new ATT&CK technique is defined *after* an MBC behavior has been defined, the preexisting MBC identifier is preserved and the new ATT&CK identifier is referenced.

ID	**X0025**
Aliases	None
Platforms	Windows
Year	2016
Associated ATT&CK Software	TrickBot

TrickBot

Trojan spyware program that has mainly been used for targeting banking sites. TrickBot is written in the C++ programming language.

Behaviors

Name	Use
Account Discovery	See ATT&CK: TrickBot - Techniques Used
Commonly Used Port	See ATT&CK: TrickBot - Techniques Used
Credentials in Web Browsers	See ATT&CK: TrickBot - Techniques Used
Credentials in Files	See ATT&CK: TrickBot - Techniques Used
Credentials in Registry	See ATT&CK: TrickBot - Techniques Used
Custom Cryptographic Protocol	See ATT&CK: TrickBot - Techniques Used
Data from Local System	See ATT&CK: TrickBot - Techniques Used
Deobfuscate/Decode Files or Information	See ATT&CK: TrickBot - Techniques Used
Disabling Security Tools	See ATT&CK: TrickBot - Techniques Used
Domain Trust Discovery	See ATT&CK: TrickBot - Techniques Used
Email Collection	See ATT&CK: TrickBot - Techniques Used
Execution through API	See ATT&CK: TrickBot - Techniques Used
File and Directory Discovery	See ATT&CK: TrickBot - Techniques Used

What is coming in the following months?

34 lines (34 sloc) | 1.04 KB

Raw | Blame | History

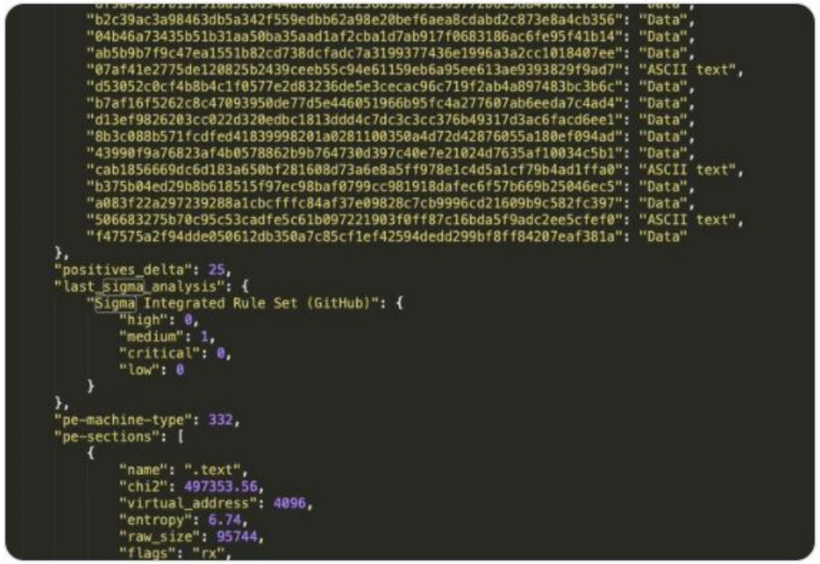
```yaml
title: Silence.EDA Detection
id: 3ceb2083-a27f-449a-be33-14ec1b7cc973
status: experimental
description: Detects Silence empireDNSagent
author: Alina Stepchenkova, Group-IB, oscd.community
date: 2019/11/01
modified: 2019/11/20
tags:
    - attack.g0091
    - attack.s0363
logsource:
    product: windows
    service: powershell
detection:
    empire:
        ScriptBlockText|contains|all:          # better to randomise the order
            - 'System.Diagnostics.Process'
            - 'Stop-Computer'
            - 'Restart-Computer'
            - 'Exception in execution'
            - '$cmdargs'
            - 'Close-Dnscat2Tunnel'
    dnscat:
         ScriptBlockText|contains|all:          # better to randomise the order
            - 'set type=$LookupType`nserver'
            - '$Command | nslookup 2>&1 | Out-String'
            - 'New-RandomDNSField'
            - '[Convert]::ToString($SYNOptions, 16)'
            - '$Session.Dead = $True'
            - '$Session["Driver"] -eq'
    condition: empire and dnscat
falsepositives:
    - Unknown
level: critical
```

Twittear

Marc Rivero López
@Seifreed

UAU, I didn't know that the #sigma rules were now integrated in @virustotal cc @cyb3rops

Traducir Tweet



7:11 p. m. · 9 may. 2020 · Twitter Web App IMG⇩

Ver actividad del Tweet

2 Retweets **9** Me gusta

Emiliano Martinez @zenitrame · 13h
En respuesta a @Seifreed @virustotal y @cyb3rops
Shhhh, don't tell anyone, coming soon ;)
1 8

Marc Rivero López @Seifreed · 12h
Coooooool
1

McAfee

Questions?

Marc Rivero López
@seifreed