



CROWDSTRIKE

클라우드스트라이크 차세대 백신
CROWDSTRIKE FALCON PREVENT

부성현 기술이사 / GREM CISSP CISA

CROWDSTRIKE KOREA

WE STOP  BREACHES



THREAT GRAPH

자동화 헌팅 엔진 HUNTING ENGINE

135 MILLION
IOA DECISIONS/MIN

7 TRILLION
EVENTS/WEEK

170+
ADVERSARIES TRACKED

THREAT GRAPH

자동화 헌팅 엔진 HUNTING ENGINE

135 MILLION
IOA DECISIONS/MIN

7 TRILLION
EVENTS/WEEK

170+
ADVERSARIES TRACKED

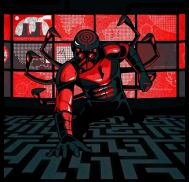
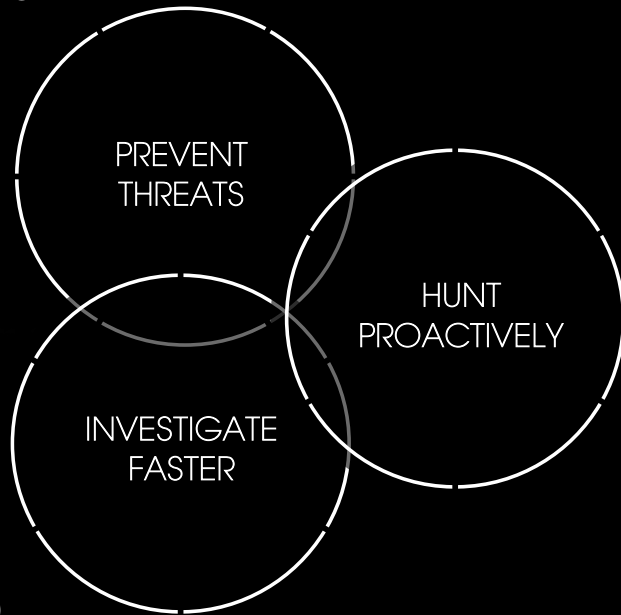
ENRICHED
DATA

ACTIONABLE
INSIGHTS

ANALYZED
DATA

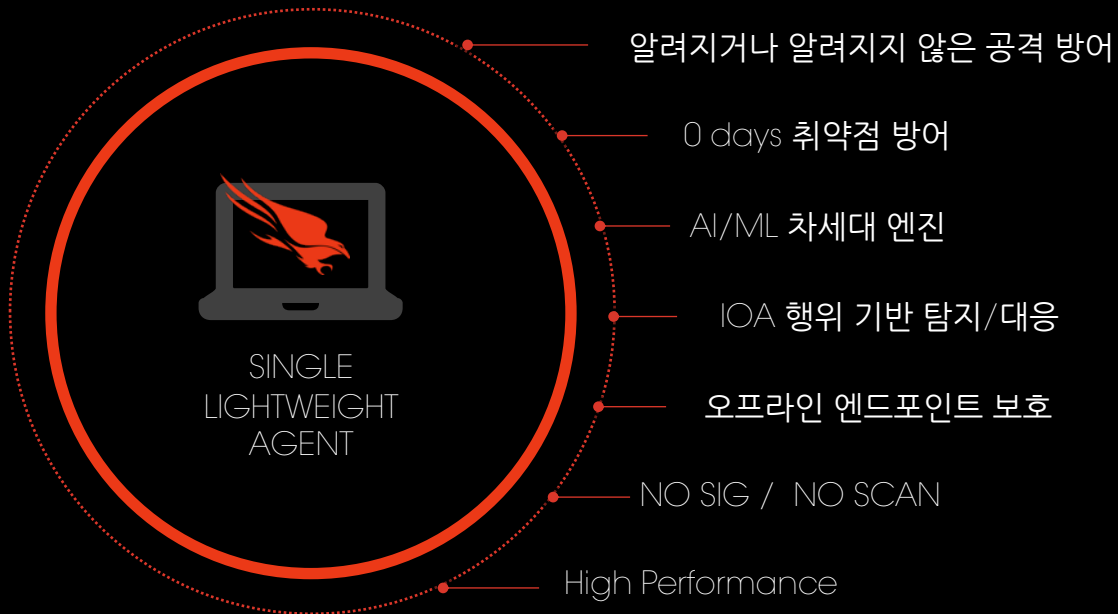
90,000

POTENTIAL BREACHES STOPPED



SINGLE LIGHTWEIGHT AGENT

단일 경량화 센서 ML BASED NEXT GEN



THE POWER
OF ONE



SINGLE LIGHTWEIGHT AGENT

단일 경량화 센서 ML BASED NEXT GEN

차별화된 차세대 백신

- 하루에도 여러 번 업데이트가 되는 레거시 백신과는 다르게 차세대 백신은 시그니처 없이 머신러닝 알고리즘으로 탐지하기 때문에 업데이트 스톱이 없음
- 최신 업데이트가 되어야 최상의 탐지율을 제공하는 레거시 백신과는 다르게 차세대 백신은 일관된 최상의 탐지율을 제공



A PROVEN SECURITY LEADER

엔드포인트 프로텍션 부문 글로벌 리더

Gartner® Magic Quadrant™ for
Endpoint Protection Platforms, May 2021

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)



Endpoint Protection Platforms



Endpoint Detection and Response Solutions

Gartner Magic Quadrant for Endpoint Protection Platforms, Paul Webber, Peter Firstbrook, Rob Smith, Mark Harris, Prateek Bhajanka 5th May 2021
This graphic is published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from CrowdStrike. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The GARTNER PEER INSIGHTS logo is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences and do not represent the views of Gartner or its affiliates. <https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms> and <https://www.gartner.com/reviews/customers-choice/endpoint-detection-and-response-solutions>



A PROVEN SECURITY LEADER

엔드포인트 프로텍션 부문 글로벌 리더

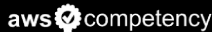
Leader In

Gartner • FORRESTER® • IDC

Validated

MITRE • AV comparatives • SE Labs

Compliance & Certifications



A PROVEN SECURITY LEADER

2022 AV-TEST MacOS 평가에서 최고 점수 달성

Falcon Pro for Mac: **Maximum Score**

AV-TEST MacOS Evaluation
for Business Users,
March 2022



CrowdStrike는 2022년 3월 기업 사용자를 위한 AV-TEST MacOS 평가에 참여한 벤더 중 오탐율 제로와 더불어 보호, 성능 및 사용성에서 **가장 높은 점수**를 얻은 **유일한 벤더**



NEXT-GEN AV FALCON PREVENT



CROWDSTRIKE FALCON
CERTIFIED AS LEGACY
AV REPLACEMENT

제공되는 가치

더 나은 보호기능 제공

침해사고 감소

사용자 생산성 향상

복잡성 제거

보안 효율성 제공



FALCON PREVENT Malware 대응

backdoor.exe

Investigator Investigator | In Progress | Comment

CS-160228-1151 | Lift Containment

Execution Details

DETECT TIME	FIRST BEHAVIOR	MOST RECENT BEHAVIOR
	Mar. 7, 2017 19:49:46	Mar. 7, 2017 20:11:35

HOSTNAME: CS-160228-1151

USER ACCOUNT: CS-160228-1151\CS_User

ASSOCIATED BEHAVIOR: High Severity Activity Prevented
This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was blocked.

1. 머신러닝에 의한 맬웨어 차단

Command Line: \\?\C:\Users\CS_User\AppData\Local\Temp\IXP000...

COMMAND LINE: C:\Users\CS_User\AppData\Local\Temp\IXP000.TMP\backdoor.exe

FILE PATH: \Device\HarddiskVolume1\Users\CS_User\AppData\Local\Temp\IXP000.TMP\backdoor.exe

SHA256: 69dc5c6e8ef3d8651591c1b108a2e236af08f2ebdc0b2cdecfae7a49efc73530

GLOBAL PREVALENCE: Common | LOCAL PREVALENCE: Common

MD5: _____

3. 탐지 뿐만 아니라 공격 이벤트에 대한 전체 흐름을 단계별로 확인



FALCON PREVENT File Less Attack 대응

SEVERITY ● High

OBJECTIVE Keep Access

TACTIC & TECHNIQUE Persistence via Accessibility Features

TECHNIQUE ID T1546.008

IOA NAME RegWriteMagnifyBypass

IOA DESCRIPTION A registry key was set to replace the magnify accessibility tool, which is often done by attackers to bypass the login screen.

- 이상 행위 탐지(IOA)엔진 / File-less attack detect
- 탐지 시 보다 세분화된 Tactic/Technique 정보 제공
- MITRE ATT&CK TID / CrowdStrike TID로 구성
- Falcon 콘솔 또는 API를 통해 MITRE 데이터 수집 가능

MITRE | ATT&CK

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	2 techniques	37 techniques	15 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (4)	Drive-by Compromise (1)	Command and Scripting Interpreter (4)	Account Manipulation (4)	Use Elevation Mechanism (2)	Abuse Elevation Control Mechanism (2)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services (1)	Archive Collected Data (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal (1)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application (1)	Exploitation for Client Execution (1)	BITS Jobs (1)	Use Token Manipulation (1)	Access Token Manipulation (4)	Credentials from Password Stores (2)	Application Window Discovery (1)	Internal Spearphishing (1)	Audio Capture (1)	Layer 7 Protocol (1)	Data Transfer Size Limits (1)	Data Destruction (1)
Gather Victim Identity Information (2)	Compromise Infrastructure (4)	External Remote Services (1)	Inter-Process Communication (1)	Boot or Logon Assistant Execution (1)	Use Token Manipulation (1)	BITS-Jobs (1)	Exploitation for Credential Access (1)	Browser Bookmark Discovery (1)	Browser Infrastructure Discovery (1)	Automated Collection (1)	Clipboard Data Encoding (2)	Exfiltration Over Alternative Protocol (1)	Data Encrypted for Impact (1)
Gather Victim Network Information (4)	Develop Capabilities (4)	Hardware Additions (1)	Native API (1)	Boot or Logon Initialization Scripts (4)	For Logon or Logon Initiation (1)	Deobfuscate/Decode Files or Information (1)	Exploitation for Credential Access (1)	Cloud Service Dashboard (1)	Remote Service Session Hijacking (2)	Data from Cloud Storage Object (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Data Manipulation (2)
Gather Victim Org Information (2)	Establish Accounts (2)	Phishing (2)	Scheduled Task/Job (4)	Browser Extensions (1)	For Logon or Logon Initiation (1)	Direct Volume Access (1)	Exploitation for Credential Access (1)	Cloud Service Discovery (1)	Remote Service Session Hijacking (2)	Data from Cloud Storage Object (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Defacement (2)
Phishing for Information (2)	Obtain Capabilities (4)	Replication Through Removable Media (1)	Shared Modules (1)	Compromise Client Software Binary (1)	Use or Modify Tools (4)	Domain Policy Modification (2)	Exploitation for Credential Access (1)	Cloud Service Discovery (1)	Remote Services (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Disk Wipe (2)
Search Closed Sources (2)	Supply Chain Compromise (2)	System Services (1)	User Execution (2)	Create Account (2)	Main Policy Modification (2)	Execution Guardrails (1)	Exploitation for Defense Evasion (1)	Domain Directory Discovery (1)	Application Through Removable Media (1)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (1)	Trusted Relationship (1)	Windows Management Instrumentation (1)	Event Triggered Execution (1)	Create or Modify System Process (4)	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	File and Directory Discovery (1)	Application Through Removable Media (1)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Firmware Corruption (1)
Search Open Websites/Domains (4)	Valid Accounts (4)		Event Triggered Execution (1)	Event Triggered Execution (1)	Hide Artifacts (2)	Hide Artifacts (2)	Hide Artifacts (2)	File and Directory Discovery (1)	Software Deployment Tools (1)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Inhibit System Recovery (1)
Search Victim-Owned Websites (1)			External Remote Services (1)	Hijack Execution Flow (1)	OS Credential Dumping (1)	OS Credential Dumping (1)	OS Credential Dumping (1)	Network Scanning (1)	Software Deployment Tools (1)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Network Denial of Service (1)
			Hijack Execution Flow (1)	Implant Container Image (1)	Indicator Removal on Host (4)	Indicator Removal on Host (4)	Indicator Removal on Host (4)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Resource Hijacking (1)
			Implant Container Image (1)	Office Application Startup (4)	Indirect Command Execution (1)	Indirect Command Execution (1)	Indirect Command Execution (1)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Scheduled Transfer (1)
			Office Application Startup (4)	Pre-OS Boot (4)	Install/Uninstall (1)	Install/Uninstall (1)	Install/Uninstall (1)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	Service Stop (1)
			Pre-OS Boot (4)	Scheduled Task/Job (4)	Masquerading (4)	Masquerading (4)	Masquerading (4)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	System Shutdown/Reboot (1)
			Scheduled Task/Job (4)	Server Software Component (2)	Modify Authentication Process (4)	Modify Authentication Process (4)	Modify Authentication Process (4)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
			Server Software Component (2)	Traffic Signaling (1)	Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
			Traffic Signaling (1)	Valid Accounts (4)	Modify Registry (1)	Modify Registry (1)	Modify Registry (1)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
			Valid Accounts (4)		Modify System Image (2)	Modify System Image (2)	Modify System Image (2)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
					Network Boundary Bridging (1)	Network Boundary Bridging (1)	Network Boundary Bridging (1)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
					Obfuscated Files or Information (1)	Obfuscated Files or Information (1)	Obfuscated Files or Information (1)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
					Pre-OS Boot (4)	Pre-OS Boot (4)	Pre-OS Boot (4)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
					Process Injection (1)	Process Injection (1)	Process Injection (1)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
					Rogue Domain Controller (1)	Rogue Domain Controller (1)	Rogue Domain Controller (1)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
					Rootkit (1)	Rootkit (1)	Rootkit (1)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	
					Signed Binary Proxy Execution (1)	Signed Binary Proxy Execution (1)	Signed Binary Proxy Execution (1)	Network Scanning (1)	Use Alternate Authentication Material (4)	Data from Local System (1)	Data Exfiltration (2)	Exfiltration Over OS Channel (1)	



FALCON PREVENT Exploit 대응

The screenshot displays the CrowdStrike Falcon Prevent interface. On the left, a process tree shows the execution flow: EXPLORER.EXE → OUTLOOK.EXE → FIREFOX.EXE → ...CONTAINER.EXE → ...P2LAUNCHER.EXE → JAVA.EXE → JAVA.EXE. The final JAVA.EXE process is highlighted with a red shield icon, indicating it was blocked. On the right, the 'Execution Details' panel provides the following information:

DETECT TIME	Jan. 11, 2022 20:26:18
HOSTNAME	SE-APA-WIN10-BL
HOST TYPE	Workstation
USER NAME	SE-APA-WIN10-BL\demo
ACTION TAKEN	Process blocked
SEVERITY	High
OBJECTIVE	Follow Through
TACTIC & TECHNIQUE	Execution via Exploitation for Client Execution
TECHNIQUE ID	T1203
IOA NAME	JavaUnusualArgs
IOA DESCRIPTION	Java executed with an unusual set of arguments. This might indicate a Java-based exploit. Review the command line.
TRIGGERING INDICATOR	Associated IOC (SHA256 on library/DLL loaded) b68befefc3a96ebcfeca749dd4d69b40f47b6b4e1de83dd3...
GLOBAL PREVALENCE	Common
LOCAL PREVALENCE	Common
IOC MANAGEMENT ACTION	None
Associated File	\Device\HarddiskVolume2\Program Files (x86)\Java\jre6\bin\java.exe

JAVA Exploit 탐지/차단



FALCON PREVENT Ransomware 대응

TYPE: Next-Gen Antivirus
CATEGORY: Cloud Machine Learning

1. 머신러닝에 의한 랜섬웨어 파일 탐지/차단

Cloud Anti-malware

Use cloud-based machine learning informed by global analysis of executables to detect and prevent known malware for your online hosts. [About levels](#)

	DISABLED	CAUTIOUS	MODERATE	AGGRESSIVE	EXTRA AGGRESSIVE
Detection					
Prevention					

Adware & PUP

Use cloud-based machine learning informed by global analysis of executables to detect and prevent adware and potentially unwanted programs (PUP) for your online hosts. [About levels](#)

	DISABLED	CAUTIOUS	MODERATE	AGGRESSIVE	EXTRA AGGRESSIVE
Detection					
Prevention					

TYPE: Behavior-Based Prevention
CATEGORY: Ransomware

2. 랜섬웨어의 행위에 대한 탐지/차단

Enable All

<p>Backup Deletion</p> <p>Deletion of backups often indicative of ransomware activity.</p> <p><input checked="" type="checkbox"/></p>	<p>Cryptowall</p> <p>A process associated with Cryptowall was blocked.</p> <p><input checked="" type="checkbox"/></p>	<p>File Encryption</p> <p>A process that created a file with a known ransomware extension was terminated.</p> <p><input checked="" type="checkbox"/></p>	<p>Locky</p> <p>A process determined to be associated with Locky was blocked.</p> <p><input checked="" type="checkbox"/></p>
<p>File System Access</p> <p>A process associated with a high volume of file system operations typical of ransomware behavior was terminated.</p> <p><input checked="" type="checkbox"/></p>	<p>Volume Shadow Copy - Audit</p> <p>Create an alert when a suspicious process deletes volume shadow copies. Recommended: Use audit mode with a test group to try allowlisting trusted software before turning on Protect.</p> <p><input checked="" type="checkbox"/></p>	<p>Volume Shadow Copy - Protect</p> <p>Prevent suspicious processes from deleting volume shadow copies.</p> <p><input checked="" type="checkbox"/></p>	



FALCON PREVENT Threat Actor 대응 (APT, e-Crime)

CROWDSTRIKE
NAMED A LEADER

The Forrester Wave:
External Threat Intelligence Services,
Q1 2021



Medium	3	Execution	28	Process Injection	23	Last
Low	2	Credential Access	13	Command Line Interface	14	Last
Informational	0	Post Exploit	13	Credential Dumping	13	Last
+Q	+Q	7 more	+Q	15 more	+Q	

<input type="checkbox"/> Select All	Update & Assign
-------------------------------------	-----------------

<input type="checkbox"/>		High	TACTIC & TECHNIQUE Machine Learning via Sensor-based ...	DETECT TIME Aug. 6, 2020 10:48:18
<div style="background-color: #e67e22; padding: 5px; display: flex; align-items: center;"> ⌵ STONE PANDA Detected </div>				
<input type="checkbox"/>		High +14 others	TACTIC & TECHNIQUE Execution via Exploitation for Client ...	DETECT TIME Aug. 6, 2020 10:44:33
<div style="background-color: #e67e22; padding: 5px; display: flex; align-items: center;"> ⌵ VOLATILE KITTEN Detected </div>				
<input type="checkbox"/>		High +5 others	TACTIC & TECHNIQUE Machine Learning via Cloud-based ML	DETECT TIME Aug. 6, 2020 10:35:47
<input type="checkbox"/>		High	TACTIC & TECHNIQUE Machine Learning via Sensor-based ...	DETECT TIME Aug. 6, 2020 10:34:23

Customers

CrowdStrike Intelligence assesses with low confidence that GRACEFUL SPIDER likely operates internally.

Victims

GRACEFUL SPIDER has targeted companies in a variety of sectors, including a targeted campaign against organizations in Africa and Europe.



**VELVET
SIGINT**



**RICOCHET
HUMINT**



**STARDUST
HUMINT**

Crimes

- Wire Fraud
- Accessing a computer without authorization for the purpose of commercial advantage and private financial gain
- Damaging a computer through the transmission of code and commands
- Conspiring to commit fraud and related activity in connection with computers
- Transmitting a demand in relation to damaging a protected computer

Monetization

- Ransom payments through cryptocurrency
- Extorting stolen data if ransom is not paid
- Monetary theft through wire fraud from victim accounts
- Likely selling payment card data via criminal marketplaces

Technical Tradecraft

GetAndGo Loader

- Distribution campaigns often use URL shorteners
- Use of HTML attachments containing links to dropper documents hosted on filesharing-themed websites
- Use of IP address geolocation filtering on landing pages and tracking of victims through links to iplogger[.]org
- The macro extracts the GetAndGo loader dynamic link library (DLL) to the %APPDATA% folder, and the appropriate DLL is extracted based on whether the Operating System
- C2 beacon to domain that typically impersonates legitimate services/companies, followed by HTTPS traffic on TCP port 443 to corresponding IP address
- Self-signed SSL certificates
- C2 servers use DNSPod[.]com name servers

ACTOR에 대한 정보 제공

- 타깃 국가 / 타깃 산업군
- 마지막 활동 시간
- 범죄 동기 / 범행 목적
- Kill Chain
- 엔드포인트 플랫폼과 자동 연계





감사합니다

CROWDSTRIKE

