퍼즐#1
엔드포인트 시큐리티, 빠진 조각은 무엇인가?

모두가 얘기하는 엔드포인트 시큐리티. 하지만 놓치고 있는 부분은 무엇일까?

오진석 기술총괄 상무

FireEye Korea SE Manager

엔드포인트 나는 이렇게 도입했다!

2004	2007	2011	2012	2015	2017	2018
FIREEYE CounterTack	TANIUM	CROWDSTRIKE	cybereason CYLANCE	*RSA2015*	Genians	AhnLab NPCORE
Tripwire	BeyondTrust	Dtex Systems	LogRhythm	Nuix	Secdo	이노티움
Verint	Check Point	Endgame	Malwarebytes	Nyotron	SecureWorks	이스트시큐리티
Ziften	Cyberbit	Fidelis	McAfee	Panda	SentinelOne	큐브피아
ZoneFox	Cynet	F-Secure	Triumfant	Promisec	Sophos	하우리
Infocyte	Digital Guardian	Invincea	Nexthink	RedCanary	TrendMicro	

엔드포인트 나는 이렇게 도입했다!

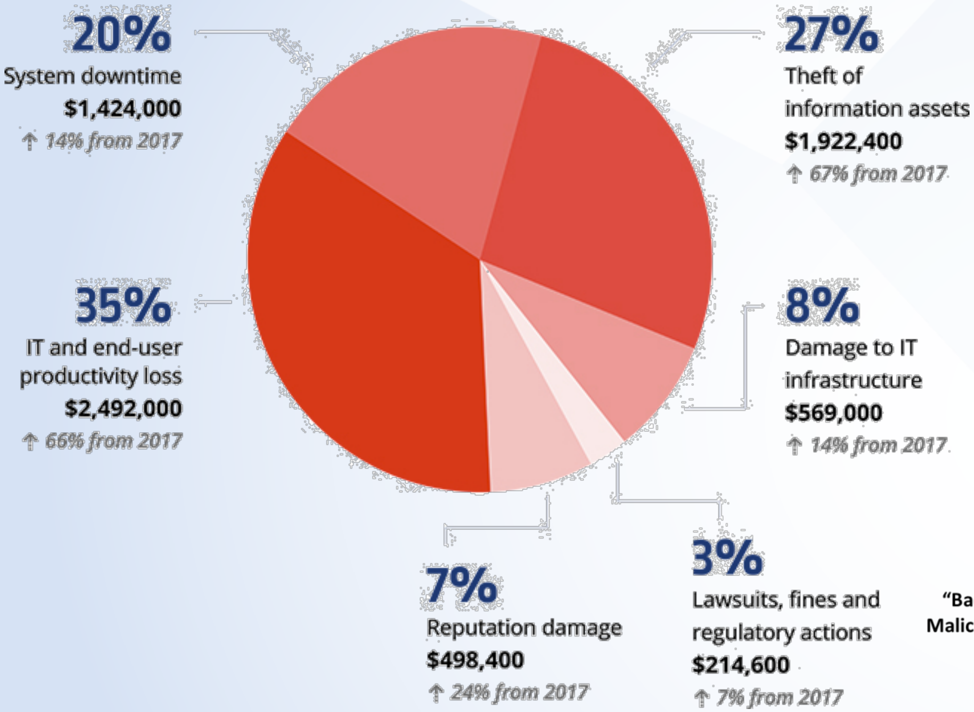
공격과 대응(방어)

CERT
보안규정관리
보안관제
보안교육
APT
FW/IPS
SPAM
보안운영
보안감사
EDR
AV
망분리
SIEM
보안정책
DLP
Reversing
암호화
NAC
코드분석

타겟팅 공격과 엔드포인트 보안

Cost of endpoint attacks

The average organization lost $7,120,000 as a result of endpoint attacks.



20%
System downtime
$1,424,000
↑ *14% from 2017*

27%
Theft of information assets
$1,922,400
↑ *67% from 2017*

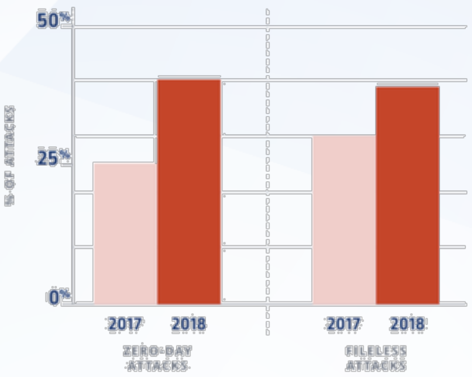
35%
IT and end-user productivity loss
$2,492,000
↑ *66% from 2017*

8%
Damage to IT infrastructure
$569,000
↑ *14% from 2017*

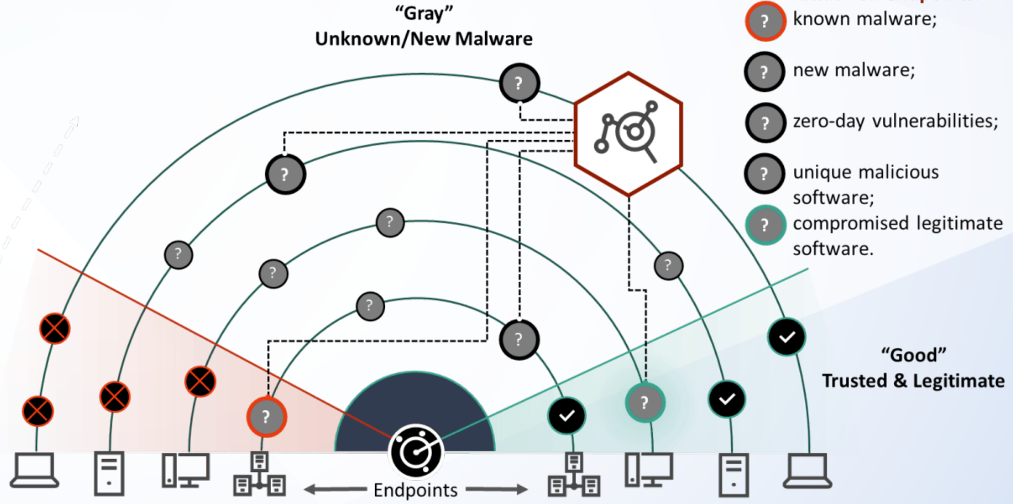
7%
Reputation damage
$498,400
↑ *24% from 2017*

3%
Lawsuits, fines and regulatory actions
$214,600
↑ *7% from 2017*

Growth in zero-day and fileless attacks

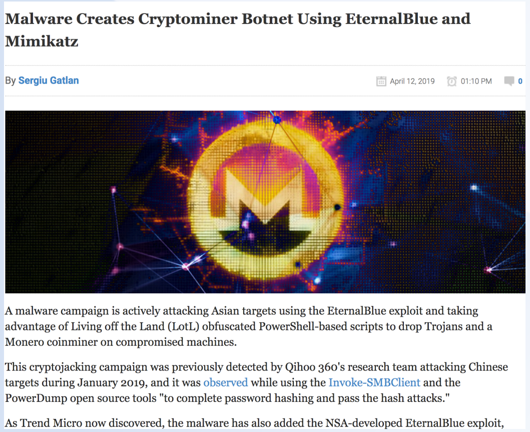


Composition of targeted attack on endpoints:



- ? known malware;
- ? new malware;
- ? zero-day vulnerabilities;
- ? unique malicious software;
- ? compromised legitimate software.

백신의 역할과 한계점



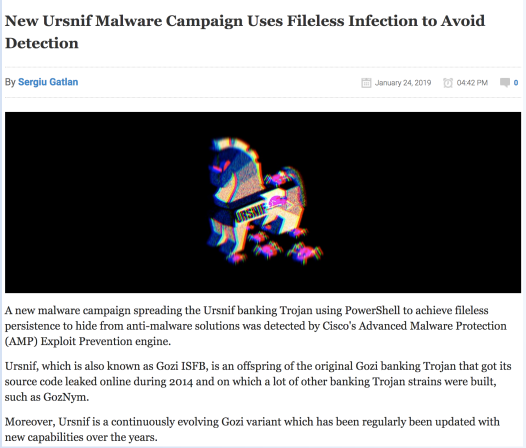
Malware Creates Cryptominer Botnet Using EternalBlue and Mimikatz

By Sergiu Gatlan April 12, 2019 01:10 PM 0

A malware campaign is actively attacking Asian targets using the EternalBlue exploit and taking advantage of Living off the Land (LotL) obfuscated PowerShell-based scripts to drop Trojans and a Monero coinminer on compromised machines.

This cryptojacking campaign was previously detected by Qihoo 360's research team attacking Chinese targets during January 2019, and it was observed while using the Invoke-SMBClient and the PowerDump open source tools "to complete password hashing and pass the hash attacks."

As Trend Micro now discovered, the malware has also added the NSA-developed EternalBlue exploit,



New Ursnif Malware Campaign Uses Fileless Infection to Avoid Detection

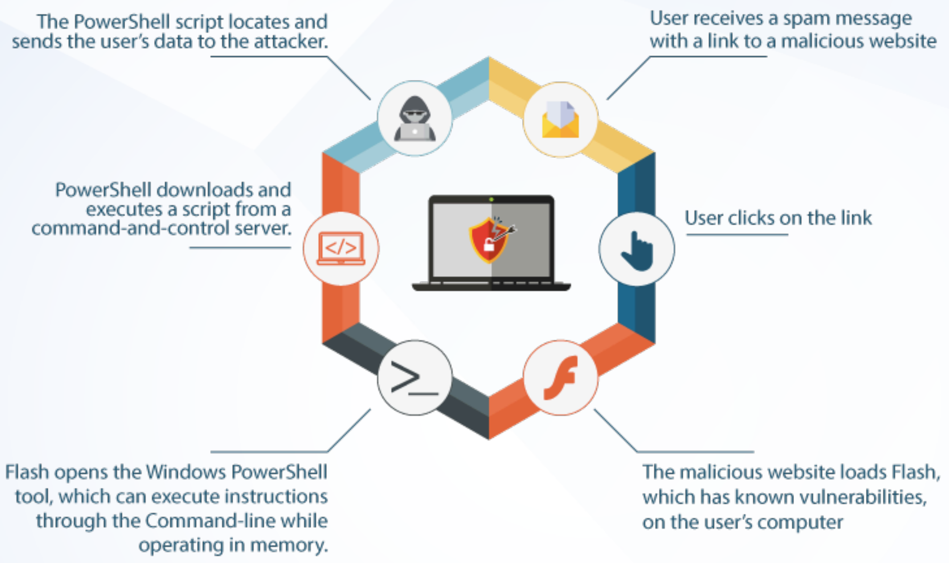
By Sergiu Gatlan January 24, 2019 04:42 PM 0

A new malware campaign spreading the Ursnif banking Trojan using PowerShell to achieve fileless persistence to hide from anti-malware solutions was detected by Cisco's Advanced Malware Protection (AMP) Exploit Prevention engine.

Ursnif, which is also known as Gozi ISFB, is an offspring of the original Gozi banking Trojan that got its source code leaked online during 2014 and on which a lot of other banking Trojan strains were built, such as GozNym.

Moreover, Ursnif is a continuously evolving Gozi variant which has been regularly been updated with new capabilities over the years.

Fileless Malware Attack Process



User receives a spam message with a link to a malicious website

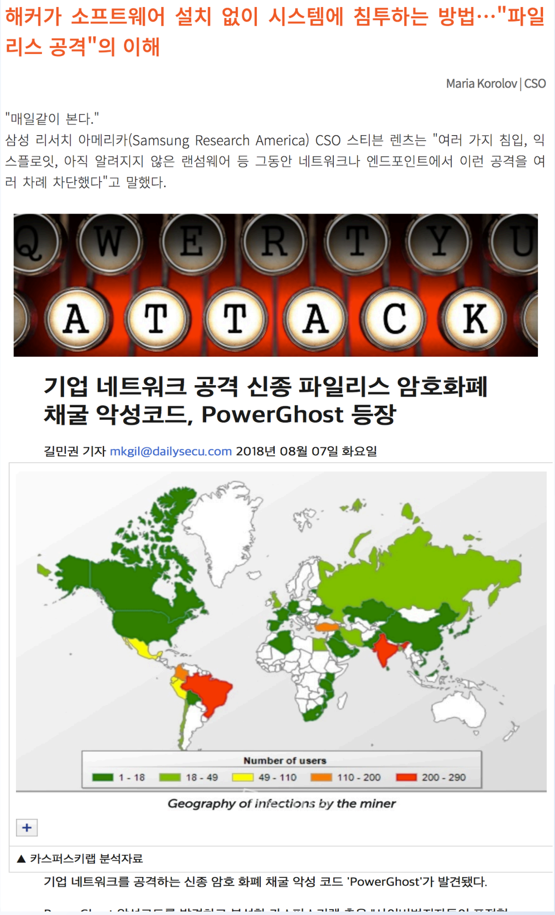
User clicks on the link

The malicious website loads Flash, which has known vulnerabilities, on the user's computer

Flash opens the Windows PowerShell tool, which can execute instructions through the Command-line while operating in memory.

PowerShell downloads and executes a script from a command-and-control server.

The PowerShell script locates and sends the user's data to the attacker.



해커가 소프트웨어 설치 없이 시스템에 침투하는 방법…"파일리스 공격"의 이해

Maria Korolov | CSO

"매일같이 본다."
삼성 리서치 아메리카(Samsung Research America) CSO 스티븐 렌츠는 "여러 가지 침입, 익스플로잇, 아직 알려지지 않은 랜섬웨어 등 그동안 네트워크나 엔드포인트에서 이런 공격을 여러 차례 차단했다"고 말했다.

기업 네트워크 공격 신종 파일리스 암호화폐 채굴 악성코드, PowerGhost 등장

길민권 기자 mkgil@dailysecu.com 2018년 08월 07일 화요일

Geography of infections by the miner

+

▲ 카스퍼스키랩 분석자료

기업 네트워크를 공격하는 신종 암호 화폐 채굴 악성 코드 'PowerGhost'가 발견됐다.

차세대 엔드포인트의 필요성

사건 이후 어떤 대응이 필요할까요?

보석상 셔터를 견고하게 변경?
센서 등을 통한 경보시스템?

셔터의 최소 높이?

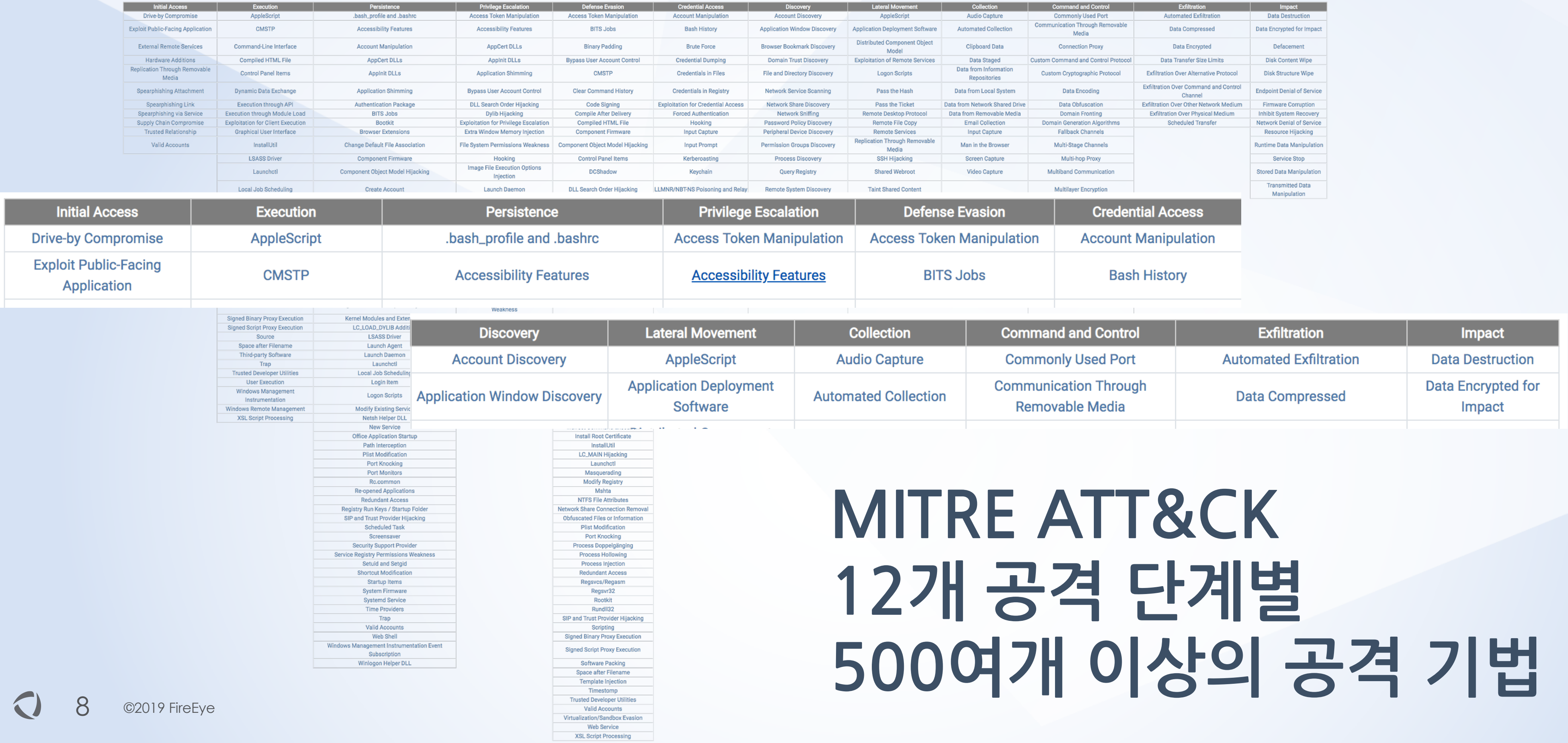
사건 이후 무엇을 분석하시겠습니까?

남녀로 보이는 듯한 두 강도
60초 안에 범행 진행해

쉽게 깨지지 않는 진열대?
사각지대 없는 CCTV?

어떤 도구로 진열대를 깬 것인지?

차세대 엔드포인트의 필요성



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History

Weakness

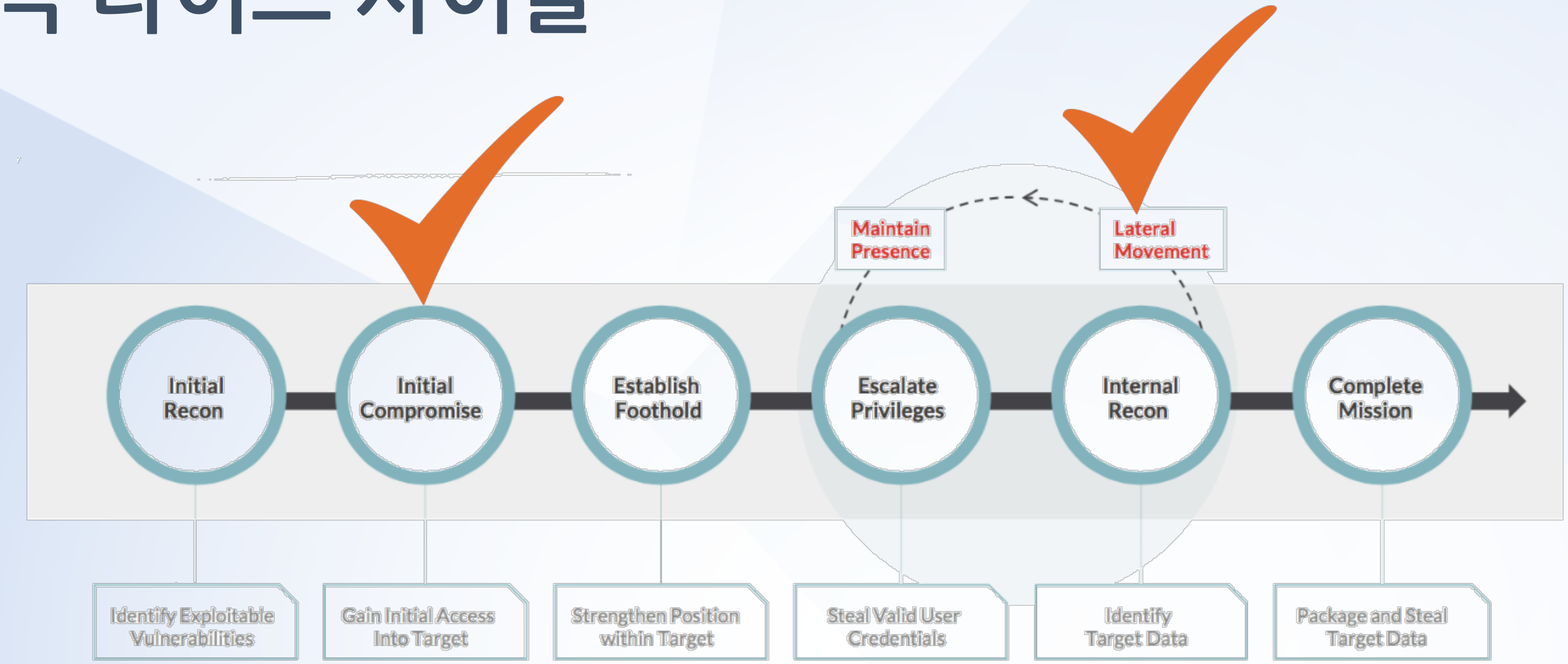
Execution	Persistence
Signed Binary Proxy Execution	Kernel Modules and Exten
Signed Script Proxy Execution	LC_LOAD_DYLIB Additi
Source	LSASS Driver
Space after Filename	Launch Agent
Third-party Software	Launch Daemon
Trap	Launchctl
Trusted Developer Utilities	Local Job Scheduling
User Execution	Login Item
Windows Management Instrumentation	Logon Scripts
Windows Remote Management	Modify Existing Servic
XSL Script Processing	Netsh Helper DLL
	New Service
	Office Application Startup
	Path Interception
	Plist Modification
	Port Knocking
	Port Monitors
	Rc.common
	Re-opened Applications
	Redundant Access
	Registry Run Keys / Startup Folder
	SIP and Trust Provider Hijacking
	Scheduled Task
	Screensaver
	Security Support Provider
	Service Registry Permissions Weakness
	Setuid and Setgid
	Shortcut Modification
	Startup Items
	System Firmware
	Systemd Service
	Time Providers
	Trap
	Valid Accounts
	Web Shell
	Windows Management Instrumentation Event Subscription
	Winlogon Helper DLL

Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact

Defense Evasion
Install Root Certificate
InstallUtil
LC_MAIN Hijacking
Launchctl
Masquerading
Modify Registry
Mshta
NTFS File Attributes
Network Share Connection Removal
Obfuscated Files or Information
Plist Modification
Port Knocking
Process Doppelgänging
Process Hollowing
Process Injection
Redundant Access
Regsvcs/Regasm
Regsvr32
Rootkit
Rundll32
SIP and Trust Provider Hijacking
Scripting
Signed Binary Proxy Execution
Signed Script Proxy Execution
Software Packing
Space after Filename
Template Injection
Timestomp
Trusted Developer Utilities
Valid Accounts
Virtualization/Sandbox Evasion
Web Service
XSL Script Processing

MITRE ATT&CK
12개 공격 단계별
500여개 이상의 공격 기법

공격 라이프 사이클


Maintain Presence
Lateral Movement
Initial Recon
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Recon
Complete Mission
Identify Exploitable Vulnerabilities
Gain Initial Access Into Target
Strengthen Position within Target
Steal Valid User Credentials
Identify Target Data
Package and Steal Target Data

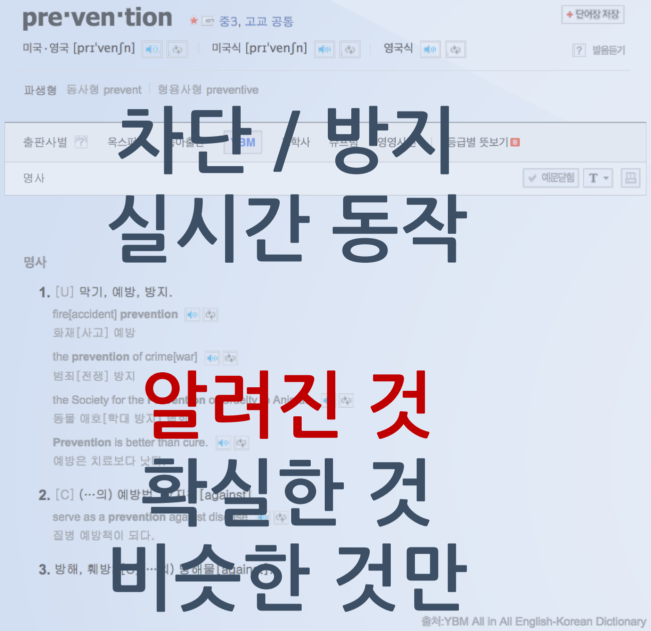
- 얼마나 많은 악성코드를 공격자가 사용할 수 있을까요?
- 공격자가 우리 기업에 엄청나게 많은 보안 시스템이 있는 것을 잘 알고 있다면 어떤 공격 방법을 쓸까요? 그래도 악성파일?

무엇에 집중할 것인가?

PREVENTION

차단 / 방지
실시간 동작

알려진 것
확실한 것
비슷한 것만
차단 가능


+ 단어장 저장
발음듣기
출판사별 옥스퍼드 동아출판 YBM 교학사 슈프림 영영사전 등급별 뜻보기
명사
예문닫힘 T

pre·ven·tion 중3, 고교 공통

미국·영국 [prɪ'venʃn] | 미국식 [prɪ'venʃn] | 영국식

파생형 동사형 prevent | 형용사형 preventive

명사

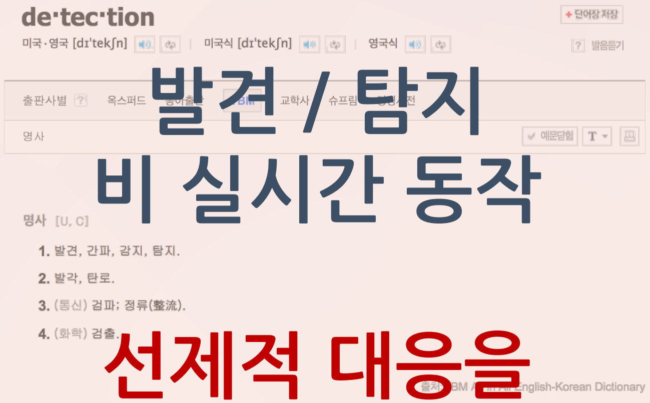
1. [U] 막기, 예방, 방지.
   fire[accident] **prevention**
   화재[사고] 예방
   the **prevention** of crime[war]
   범죄[전쟁] 방지
   the Society for the **Prevention** of Cruelty to Animals
   동물 애호[학대 방지] 협회
   Prevention is better than cure.
   예방은 치료보다 낫다.
2. [C] (…의) 예방법, 방지책 [against]
   serve as a **prevention** against disease
   질병 예방책이 되다.
3. 방해, 훼방; [C] (…의) 방해물[against].

출처:YBM All in All English-Korean Dictionary

DETECTION

발견 / 탐지
비 실시간 동작

선제적 대응을
위한 분석/확인
정상으로 보여지는
공격 활동 발견



de·tec·tion

미국·영국 [dɪ'tekʃn] | 미국식 [dɪ'tekʃn] | 영국식

명사 [U, C]

1. 발견, 간파, 감지, 탐지.
2. 발각, 탄로.
3. (통신) 검파; 정류(整流).
4. (화학) 검출.

출처:YBM All in All English-Korean Dictionary

RESPONSE

대응 / 반응
새로운 접근

발견된 공격활동에
대한 가시성 확보
차단 및 탐지가
부족한 부분 대응

+ 단어장 저장
발음듣기
출판사별 옥스퍼드 동아출판 YBM 교학사 슈프림 영영사전 등급별 뜻보기
명사
예문닫힘 T

re·sponse 중3, 고교 공통, 고교 영어1, 고교 영어2

미국식 [rɪ'spɑːns] | 영국식 [rɪ'spɒns]

파생형 동사형 respond | 형용사형 responsive | responseless

유의어/반의어 [명사] answer, return, reply, … 더보기

명사 (pl. –spons·es[–iz])

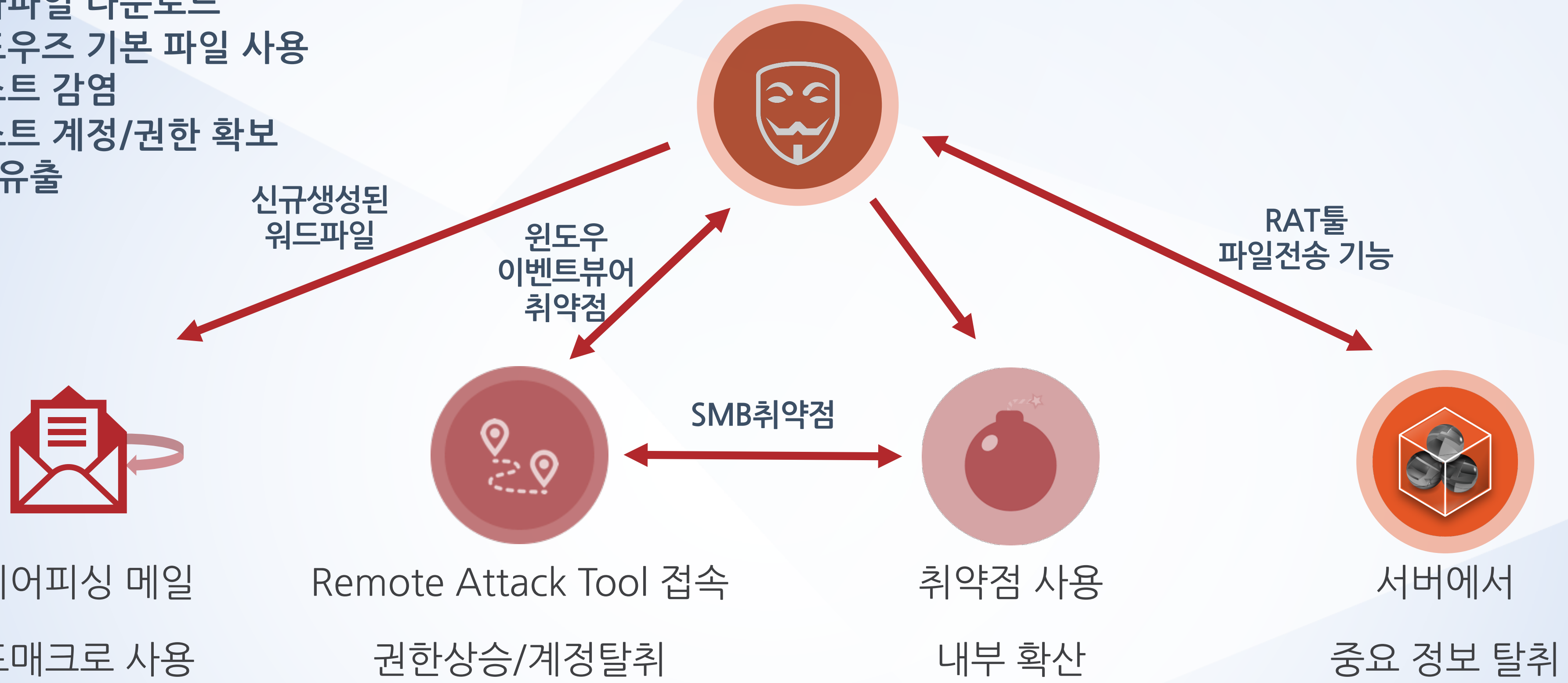
1. 응답, 대답; [U, C]반응, 반향[to, from].
   make a **response**
   답하다.
2. [U, C] (생물·심리) (자극에 대한) 반응.
   response to stimuli
   자극에 대한 반응
3. (교회) 답창, 답창가(歌); 응답 송가.
4. (카드놀이) 리스폰스(파트너의 비드(bid)에 대한 응답 비드).
5. (전자) 리스폰스, 응답.

출처:YBM All in All English-Korean Dictionary

공격자의 관점에서의 공격 데모

공격의 개요

- 1개의 피싱 메일(첨부파일)
- 4개의 추가파일 다운로드
- 6개의 윈도우즈 기본 파일 사용
- 2대의 호스트 감염
- 2대의 호스트 계정/권한 확보
- 주요 정보 유출



신규생성된 워드파일

윈도우 이벤트뷰어 취약점

RAT툴 파일전송 기능

SMB취약점

스피어피싱 메일

워드매크로 사용

Remote Attack Tool 접속

권한상승/계정탈취

취약점 사용

내부 확산

서버에서

중요 정보 탈취

이런 상황에서 어떤 대응을 할 것인가?

- 방화벽에서 알려진 악성 IP간 통신 이벤트 발생
- 다수의 백신에서 악성코드 탐지 이벤트 발생
- IPS에서 내부 시스템에 대한 공격 이벤트 발생
- Netflow 비정상 트래픽 관련 이벤트 발생
- 사용자가 이메일 첨부파일을 확인 한 이후 의심스러운 시스템 이벤트 발생
- SOC팀이나 SIEM장비에서 다수의 이벤트 발생