# Understanding Your Opponent : Attack Profiling

**25-26, August 2016, HITB GSEC, Singapore**

Moonbeom Park(Deputy General Researcher, TTPA)[1], Yongjun Park(Manager, FSI-CERT)[2]

## 1. Abstract

Through various incident response and malware analysis, attacker were using similar attack method and reusing their code for different incidents. The analysis for common points and relations between attacks can help us to better understand the purpose and tactics of attackers for more effective response.

Attack profiling is a valuable method for figuring out the motives of attacker, sharing threat intelligence and preparing response methods for expected future incident.

This profiling can be performed based on not only IP and Code, but also actor's tactics, technics, mistake and any information used in operation.

This document includes multifaceted analysis against incidents targeted government agencies, media outlets, broadcasting services, critical infrastructure and financial sector. And it will explain approach and method for attack profiling.

## 2. Attack Profiling Method and Factor

[1] neotra@gmail.com
[2] ric3box@gmail.com

## 2.1 Tactics

Actor set up their strategy first, and then performs operation according to the tactics to achieve their goal of cyber attack. They plan tactics likes, “How could I compromise target system”, “How could I gather information about target and choice best way to apply it for more effective attack”.

For example, to compromise target system and entry PC in network, attacker use spear-phishing with E-mail. It include malicious code, document and 0-day vulnerability. In this case, below factors could be used to understand actor’s tactics and identify attacker.

- Content of E-mail(Resume, Business Proposal, Information Sharing, Industrial Knowledge and etc)
- Document Type(DOC, PPT, Local Document File, HTML, JS and etc)
- Sender E-mail address and Server
- Receiver(Targeted Address and Anonymous)

Also it’s possible looking into what information they had for the attack to forecast attacker’s goal, target and next plan. Attacker gathered data related with target on preparing step by buying personal data at black market, searching Google and putting the pieces of public website of target.

If response team can find out the source of this information, they can utilize it for incident investigation to analyze details of incident. Also, if they can forecast next incident and target based on result of tactics profiling, it can help to invest resource in particular area and enforce monitoring to prevent damage of attack.

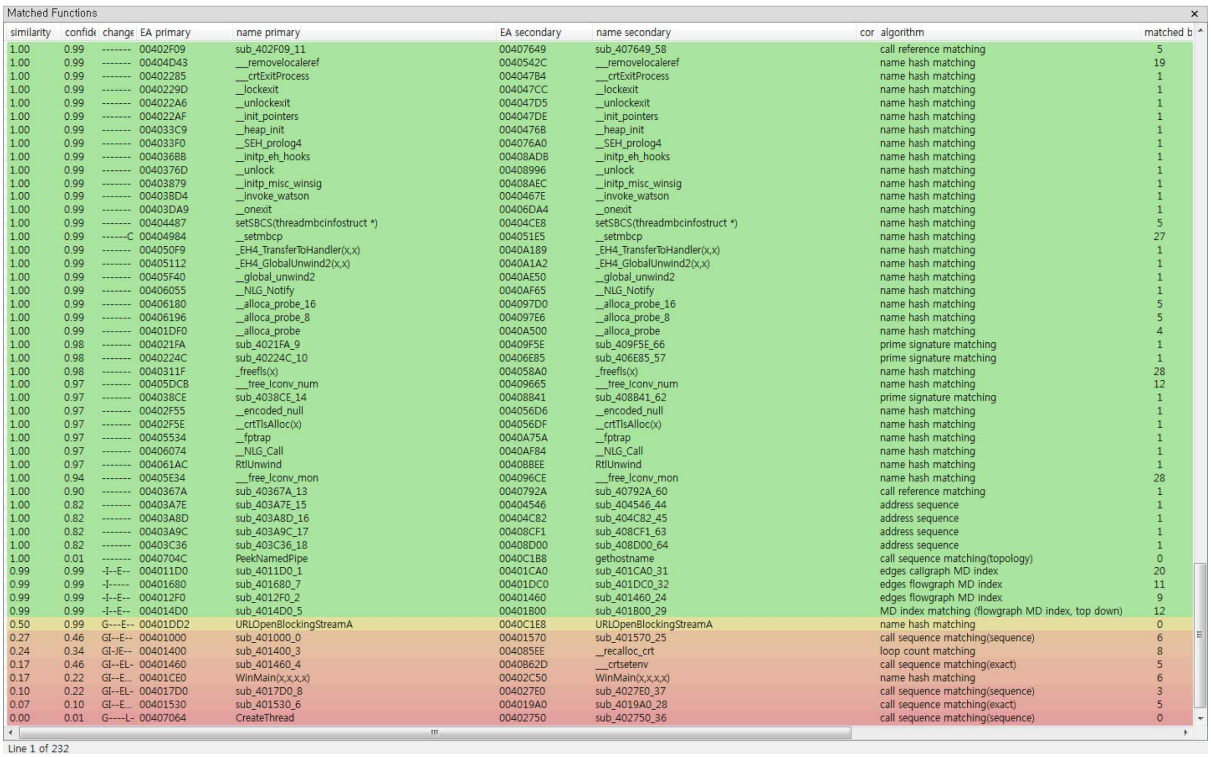
## 2.2 Code

Comparing code of malware is primarily using for profiling. It can calculate similarity between different malware and binary. The result of similarity can figure out that different incidents were operated by same actor and those incidents are connected. It means that it can help to understand not only an incident, but also full operation of cyber attack.

The method for code profiling is extracting traits from binary file. Practical traits are like name of function, particular API, string of path and command execution.

PE is also useful for comparing different binary. Code-singing, compile data, debug info, PDB and any information in PE can be a factor for code profiling.

To compare binaries with code, similarity can calculate by Diff tool. It will print diff result such as, similarity, matched functions and code graph. It can find out that actor built mutations from original malware, and reuse a part of function for another incident.


Matched Functions

| similarity | confide | change | EA primary | name primary | EA secondary | name secondary | cor | algorithm | matched b |
|---|---|---|---|---|---|---|---|---|---|
| 1.00 | 0.99 | ------- | 00402F09 | sub_402F09_11 | 00407649 | sub_407649_58 | | call reference matching | 5 |
| 1.00 | 0.99 | ------- | 00404D43 | __removelocaleref | 0040542C | __removelocaleref | | name hash matching | 19 |
| 1.00 | 0.99 | ------- | 00402285 | __crtExitProcess | 004047B4 | __crtExitProcess | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 0040229D | _lockexit | 004047CC | _lockexit | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 004022A6 | _unlockexit | 004047D5 | _unlockexit | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 004022AF | __init_pointers | 004047DE | __init_pointers | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 004033C9 | __heap_init | 0040476B | __heap_init | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 004033F0 | __SEH_prolog4 | 004076A0 | __SEH_prolog4 | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 004036BB | __initp_eh_hooks | 00408ADB | __initp_eh_hooks | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 0040376D | _unlock | 00408996 | _unlock | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 00403879 | __initp_misc_winsig | 00408AEC | __initp_misc_winsig | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 00403BD4 | __invoke_watson | 0040467E | __invoke_watson | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 00403DA9 | __onexit | 00406DA4 | __onexit | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 00404A87 | setSBCS(threadmbcinfostruct *) | 00404CE8 | setSBCS(threadmbcinfostruct *) | | name hash matching | 5 |
| 1.00 | 0.99 | ------C | 00404984 | __setmbcp | 004051E5 | __setmbcp | | name hash matching | 27 |
| 1.00 | 0.99 | ------- | 004050F9 | _EH4_TransferToHandler(x,x) | 0040A189 | _EH4_TransferToHandler(x,x) | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 00405112 | _EH4_GlobalUnwind2(x,x) | 0040A1A2 | _EH4_GlobalUnwind2(x,x) | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 00405F40 | __global_unwind2 | 0040AE50 | __global_unwind2 | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 00406055 | __NLG_Notify | 0040AF65 | __NLG_Notify | | name hash matching | 1 |
| 1.00 | 0.99 | ------- | 004061B0 | __alloca_probe_16 | 004097D0 | __alloca_probe_16 | | name hash matching | 5 |
| 1.00 | 0.99 | ------- | 00406196 | __alloca_probe_8 | 004097E6 | __alloca_probe_8 | | name hash matching | 5 |
| 1.00 | 0.99 | ------- | 00401DF0 | __alloca_probe | 0040A500 | __alloca_probe | | name hash matching | 4 |
| 1.00 | 0.98 | ------- | 004021FA | sub_4021FA_9 | 00409F5E | sub_409F5E_66 | | prime signature matching | 1 |
| 1.00 | 0.98 | ------- | 0040224C | sub_40224C_10 | 00406E85 | sub_406E85_57 | | prime signature matching | 1 |
| 1.00 | 0.98 | ------- | 0040311F | _freefls(x) | 004058A0 | _freefls(x) | | name hash matching | 28 |
| 1.00 | 0.97 | ------- | 00405DCB | __tree_lconv_num | 00409665 | __tree_lconv_num | | name hash matching | 12 |
| 1.00 | 0.97 | ------- | 004038CE | sub_4038CE_14 | 00408B41 | sub_408B41_62 | | prime signature matching | 1 |
| 1.00 | 0.97 | ------- | 00402F55 | __encoded_null | 004056D6 | __encoded_null | | name hash matching | 1 |
| 1.00 | 0.97 | ------- | 00402F5E | __crtTlsAlloc(x) | 004056DF | __crtTlsAlloc(x) | | name hash matching | 1 |
| 1.00 | 0.97 | ------- | 00405534 | __fptrap | 0040A75A | __fptrap | | name hash matching | 1 |
| 1.00 | 0.97 | ------- | 00406074 | __NLG_Call | 0040AF84 | __NLG_Call | | name hash matching | 1 |
| 1.00 | 0.97 | ------- | 004061AC | RtlUnwind | 00408BEE | RtlUnwind | | name hash matching | 1 |
| 1.00 | 0.94 | ------- | 00405E34 | __free_lconv_mon | 004096CE | __free_lconv_mon | | name hash matching | 28 |
| 1.00 | 0.90 | ------- | 0040367A | sub_40367A_13 | 0040792A | sub_40792A_60 | | call reference matching | 1 |
| 1.00 | 0.82 | ------- | 00403A7E | sub_403A7E_15 | 00404546 | sub_404546_44 | | address sequence | 1 |
| 1.00 | 0.82 | ------- | 00403A8D | sub_403A8D_16 | 00404C82 | sub_404C82_45 | | address sequence | 1 |
| 1.00 | 0.82 | ------- | 00403A9C | sub_403A9C_17 | 00408CF1 | sub_408CF1_63 | | address sequence | 1 |
| 1.00 | 0.82 | ------- | 00403C36 | sub_403C36_18 | 00408D00 | sub_408D00_64 | | address sequence | 1 |
| 1.00 | 0.01 | ------- | 004070AC | PeekNamedPipe | 0040C1B8 | gethostname | | call sequence matching(topology) | 0 |
| 0.99 | 0.99 | -I--E-- | 004011D0 | sub_4011D0_1 | 00401CA0 | sub_401CA0_31 | | edges callgraph MD index | 20 |
| 0.99 | 0.99 | -I----- | 00401680 | sub_401680_7 | 00401DC0 | sub_401DC0_32 | | edges flowgraph MD index | 11 |
| 0.99 | 0.99 | -I--E-- | 004012F0 | sub_4012F0_2 | 00401460 | sub_401460_24 | | edges flowgraph MD index | 9 |
| 0.99 | 0.99 | -I--E-- | 004014D0 | sub_4014D0_5 | 00401B00 | sub_401B00_29 | | MD index matching (flowgraph MD index, top down) | 12 |
| 0.50 | 0.99 | G---E-- | 00401DD2 | URLOpenBlockingStreamA | 0040C1E8 | URLOpenBlockingStreamA | | name hash matching | 0 |
| 0.27 | 0.46 | GI--E-- | 00401000 | sub_401000_0 | 00401570 | sub_401570_25 | | call sequence matching(sequence) | 6 |
| 0.24 | 0.34 | GI-JE-- | 00401400 | sub_401400_3 | 004085EE | __recalloc_crt | | loop count matching | 8 |
| 0.17 | 0.46 | GI--EL- | 00401460 | sub_401460_4 | 0040B62D | __crtsetenv | | call sequence matching(exact) | 5 |
| 0.17 | 0.22 | GI--E... | 00401CE0 | WinMain(x,x,x,x) | 00402C50 | WinMain(x,x,x,x) | | name hash matching | 6 |
| 0.10 | 0.22 | GI--EL- | 004017D0 | sub_4017D0_8 | 004027E0 | sub_4027E0_37 | | call sequence matching(sequence) | 3 |
| 0.07 | 0.10 | GI--E... | 00401530 | sub_401530_6 | 004019A0 | sub_4019A0_28 | | call sequence matching(exact) | 5 |
| 0.00 | 0.01 | G----L- | 00407064 | CreateThread | 00402750 | sub_402750_36 | | call sequence matching(sequence) | 0 |

Line 1 of 232

<Matched Functions with IDA + BinDiff>

Sometimes attacker leaves their signature in the binary on purpose. In this case, they usually intent to notice who is an actor. On the other hand, some incident leave particular characteristic by an attacker's mistake. For example, in some incidents, malware has debug information likes PDB path in PE, because malware developer configures debug option for released malware. This information can help to guess actor's system and environment.

## 2.3 Server and IP

Incident with malware usually have malware landing page, redirect server and C&C. Analyst can extract IP from static and dynamic analysis of malware or during compromised system investigation.

Actor usually use same server for several incidents in a similar period. Also actor use same server on several step of incident procedure. For instance, they can use a compromised server for scanning target network, download configuration file and exploit kit admin.

Attacker try to exploit a server as much as they can(but, below the detected). Because acquiring server need a cost and effort to gain compromised server with vulnerability. For these reason, used server and IP can profiled for comparing different incident.

## 2.4 Other Factors

For practical incident response, even a bit of data could help to profile TTP of attacker. It's not only technical data, also cultural thing and resource for social engineering. For example, language and sentence are also using for profiling factor such as, language in binary string, e-mail content and resource in.

Tone of sentence can help to figure out that actor try to pretend to citizen in target country. Even actor and victim are belonging to same language area, difference in grammar and nuance are useful tracing the actor nationality.

Tools using to compromise target system are another profiling factor. Actors usually use same tools and their own script for attack likes Webshell, scanning tools, injection and spoofing tools.

Also, they acquire C&C server by exploiting same vulnerability and tools with compromised weak website and open server. Figuring out these attack patterns are useful to understand attack procedure and tactics.

## 3. Case Study

### 3.1 DDoS Financial Service

- Actor : DD4BC(DDoS for Bitcoin)
- Case : Attacked Banks and Securities In South Korea

DD4BC is a famous DDoS group who attacked many countries and various industries. Their attack procedure is “Initial DDoS(NTP, SSDP, other Amplification and Reflection DDoS)” and then “Sending Black Mail(Asking Bitcoin and warning massive DDoS bigger than Initial attack)”

In this case, they operated DDoS on every Friday target to a financial institution during several weeks. To figure out their plan and next target is most important action for response and reducing risk.

Best countermeasure for DDoS is that target system doesn’t affect by attack and prove there is no damage by their attack. It makes attacker will disappoint and change a target to others. Incident response team has to find next target to reinforce monitoring in certain range and to defense of target system.

Sender : dd4bc@openmailbox.org, dd4bc@outlook.com, dd4bc@inseen.is, dd4bct@gmail.com ,dd4bcteam@keemail.me

Hello,

To introduce ourselves first:
http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks/
http://bitcoinbountyhunter.com/bitalo.html
http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info

Or just google "DD4BC" and you will find more info.
So, it's your turn!

All your servers are going under DDoS attack unless you pay xx Bitcoin.
Pay to

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps.

Right now we are running small demonstrative attack on 2 of your IPs:

Don't worry, it will not be hard and will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have xx BTC at the moment, so we are giving you 24 hours to get it and pay us.

Find the best exchanger for you on howtobuybitcoins.info or localbitcoins.com

<Black Mail from DD4BC>

They have attacked many countries[3] and various industries[4] since 2014. It means they need an information source to make a target list using their worldwide DDoS operation.

To figure out their next plan and information source, response team performed analyzing current target company and comparing previous targets.

In conclusion, DD4BC attack to financial institutions in South Korea was based on a company list in Wikipedia and Google Search. It's hard to convince that they

[3] US, UK, China, Japan, German, Swiss, Korea and other country
[4] Government, Agency, Financial Service, Online Gaming, Media and Retail

choose their target using the information for all their operation. But, only in this case, practical target list were matched with Wikipedia and Google Search.

In accordance with this result, response team noticed a warning following company in the list, and reinforces monitoring, configure their system to prepare DDoS attack.

### 3.2 Data Leaked blue print of power plant

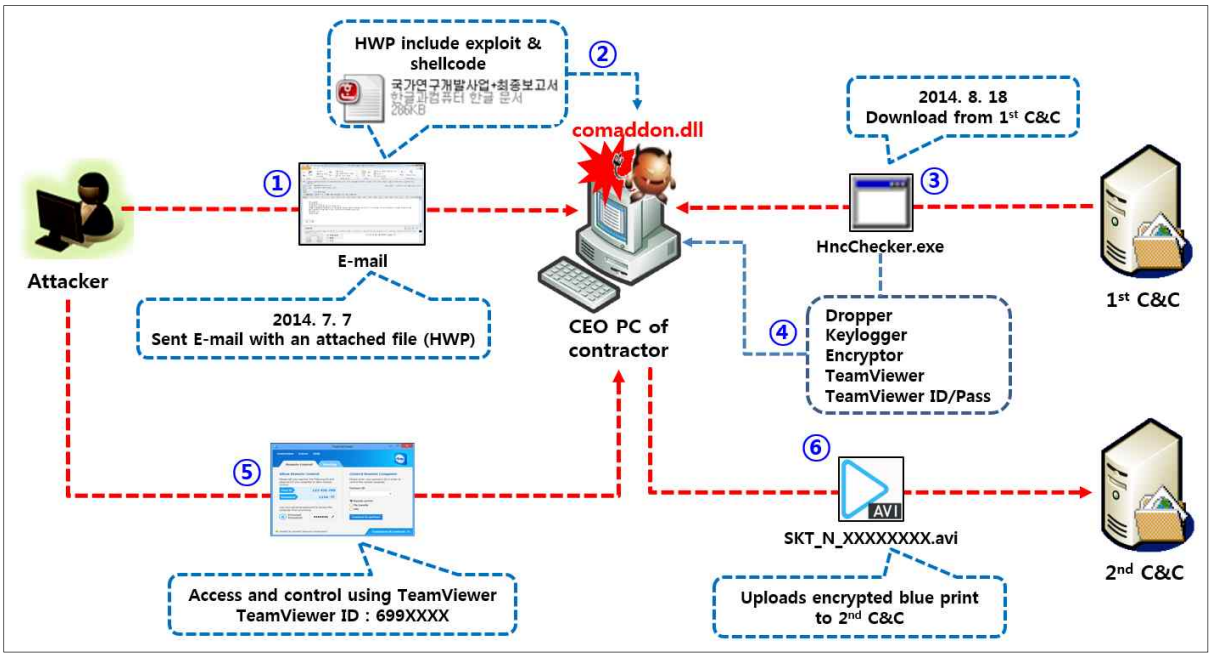
- Actor : North Korean cyber warfare
- Case : Hacked and leaked blue print of nuclear power plant In South Korea

This is spear phishing attack method using vulnerability of Korean word processor.

This method requires to use zero-day vulnerability in HWP word processor which is installed in most of South Korean PC, just like Microsoft Windows. The company, one that made this HWP word processor, released the API of their program in few years ago.

Also this program is installed in South Korean government and state-owned company. Beside MS office, this is primary program to create document in government sector.

This method is used in Dec 2014, targeting South Korean nuclear power plant hacking. The blue print is leaked.




First, Attacker use VPN service in China to login Korean free email service. They create email account and they are ready to go.

Attacker send an email at 7th, July, 2014 that has HWP file attached to South Korean nuclear power plant cooperative company's CEO. And the title of email is "[emergency] please read nuclear power plant stops due to malfunction in module".

CEO opens up the attached file, then infected. His PC is online. Malicious code "comaddon.dll" was injected and executed with "explorer.exe" process. And then, the PC access the 1st C&C server in UK and additionally downloaded "HncChecker.exe" and installed.

When this 5 other malicious code is installed, the CEO's PC has "TeamViewer" program, and attacker access this PC using TeamViewer client program. Steal nuclear power plant blue print document and compress the file with password.

And then, upload the encrypted file to 2nd C&C server somewhere in South Korea's capital.

## 4. Conclusion

Attacking profiling is not only restricted to analyze technical data. It's a process assembling and analyzing whole piece of incident and attack. We hope through this document and presentation, attendees will better understand how to analyze an attack and how to figure out that it's connected to other incidents.

[We talked more interesting and practical profiling case at the conference]

## Biography:

Moonbeom Park, a deputy general researcher in TTPA (Trusted Third Party Agency), has 9 years of experience in hacking analysis, forensic, research on hacking technic, profiling hacking source. He had presentations in various international security conference such as TROOPERS, Ekoparty, HITCON, VXCON and RedPill.

Yongjun Park, a manager in FSI-CERT, in charge of Incident Response and Threat Intelligence for Financial Industry in Korea. He has experienced Security Testing, Mobile Security, Penetration Test, Malware Analysis, Incident Response and Security Management for 9 Years.