(U) Discovery SIGINT Targeting Scenarios and Compliance

TOP SECRET//SI//REL TO USA, FVEY

(U//FOUO) SIGINT targeting scenarios with NTOC Oversight and Compliance (NOC) and NSA's Office of General Council (OGC) guidance feedback while performing discovery in V252. This will be a running list of Q&A. Please link/included memorialized copies of all related communications for each scenario to ensure integrity of this list.

Contents

[edit] Targeting Scenarios

[edit] (TS//SI/REL) Querying on Fingerprints

When using fingerprints that strongly suggest malicious activity, what defeats are needed, if any?

NOC/OGC RESPONSE: Fingerprints are okay to task on. If there is a 51%+ confidence that it is a foreign malicious method and no other information contradicts that theory, you may task with no defeats. Otherwise, defeat(s) or other selectors are required to minimize potential US/FVEYs hackers. No querying may be made to 'prove US origin' of hacking activity. There must be evidence/information that suggest it is foreign. (Source #001)

[edit] (TS//SI//REL) Known foreign malicious actor

Are any defeats needed when querying against a Known foreign malicious actor?

No defeats are needed when it is a known foreign malicious actor. (Source #002)

NOC RESPONSE: If the foreign IP is consistently associated with malicious cyber activity against the U.S., so, tied to a foreign individual or organization known to direct malicious activity our way, then there is no need to defeat any to, from, or about U.S. Persons. This is based on the description that one end of the communication would always be this suspect foreign IP, and so therefore any U.S. Person communicant would be incidental to the foreign intelligence task. In fact, you would very likely see a U.S. Person in the "TO" as a victim of spear-phishing or other campaigns, or as a "FROM" for beaconing or exfiltration activity. If, however, you believe there is a circumstance where the task will give you U.S. Persons at both ends, then I've misunderstood the description and would need more information. (Source #003)

OGC RESPONSE: OGC agrees. Please note that any USP collection obtained via targeting the selector will constitute incidental collection and any USP information would need to be minimized per USSID 18. Also, please be aware that any targeting of a foreign selector solely for the purpose of obtaining USP comms, constitute improper reverse targeting. (Source #003)

[edit] (TS//SI//REL) Two-way FVEYs defeat

Is it a free-for-all when using a two-way FVEYs defeat?

NOC/OGC RESPONSE: YES, no problem. (Source #001)

As a clarification though...querying on a known US/FVEYs selector (even with defeats) will still be reported as a violation. Example, querying on a US person's name, email address, IP address, etc. Even though you would receive 0 results...you still targeted a US person.

[edit] (TS//SI//REL) Unknowingly targeting a US person

I screwed up...the selector had a strong indication of being foreign, but it turned out to be US...now what?

NOC/OGC RESPONSE: With all querying, if you discover it actually is US, then it must be submitted and go in the OGC quarterly report...'but it's nothing to worry about'. (Source #001)

[edit] (TS//SI//REL) Potential for US-US comms

I'm still worried about a selector in which I don't have 100% confidence of it's foreignness...95% confident for the sake of argument. But, I don't want to miss out on potential communication by using a FVEYs defeat. What happens if My selector ends up being US, and I potentially get US to US comms?

NOC/OGC RESPONSE: The SIGINT system does not have the capability to collect US-US comms. (Source #001)

[edit] (TS//SI//REL) Targeting an un-registered URI

While reversing a piece of malware that came into NIPRNet, we come across a call-back to an unregistered URI. We do not know foreignness nor server location it will eventually resolve to. What are our options in tasking that selector?

NOC/OGC RESPONSE: If there is no information to suggest it is a legitimate US used site, assume foreign. If at all possible, use selectors to just focus on activity (i.e. a specific URL or file name). If you discover it actually is US, then it must be submitted and go into OGC's quarterly report...but it's nothing to worry about. (Source #001)

[edit] (TS//SI//REL) Randomly generated URIs

We frequently run across randomly generated URI in malware, DNS lookups, get request, etc. Given that the randoms indicates obfuscation, and obfuscation many times indicates malicious intent...what are our targeting options?

NOC/OGC RESPONSE: Random looking URIs can be treated as malicious unless there is contradictory information otherwise. Same applies to the foreignness of said URI...assume foreignness unless there is contradictory information otherwise. (Source #001)

[edit] (TS//SI//REL) Querying against US systems

Many foreign actors utilize US based servers/services for things like Facebook, GMail, Twitter, etc. If we 'know' a foreign actors screename/login for said US service, can we query for related traffic to/from the said US server?

NOC/OGC RESPONSE: If they are a foreign target using the account from a foreign location, then it may be fine. But if you're actually having to target the Twitter server more broadly, then probably not. NSA may target via EO 12333 a DNI selector which is confirmed foreign. (Source #003) Okay to use XKS micro-plugins (for example) that query against Facebook, GMail, Twitter, etc. IF screename/username is believed to be foreign. This is sticky though, if you 'guess' foreign and it's not, then it is a serious violation. Try to minimize to 'post' for example to filter out non-pertinent comms. (Source #001)

NOC response: Yes, you may task that domain if it was established for and used only by the foreign target, believed to be operating from an overseas location. If there is any possibility that others had previously established or could currently be using the domain, then your task must include an "and" that defeats any known U.S. Person use of the site and limits the task to only the communications that would be generated by the foreign targeted group via that domain. So if there is an entry port or protocol unique to the group, that would be an appropriate "and". Once tasked, if the collection reveals activity by U.S. Persons that is not simply incidental to the foreign intelligence task, than additional defeats must be implemented. If there is no foreign intelligence activity as expected, you would have to de-task. (Source #003)

Even though XYZcommuncation in Chicago may 'own' the equipment, a foreign actor may be 'leasing' space. What is the determining factor for 'foreign'?

NOC response: I don't know the full realm of possibilities here, but you must have either intelligence, law enforcement, commercial, or open source information denoting that the establishment and use of that webspace is by the foreign target. (Source #003)

OGC response: OGC agrees. However, it is essential that the TOPI be able to establish the foreignness of the webspace and that the defeats are sufficient to prevent any overcollect. (Source #003)

Since we can do the above, what proof would we need of the leaser being foreign…just the domain registration info from open source?

NOC response: If the registration information is explicit enough to link to your foreign target, this should be adequate. Otherwise, you'll need additional corroborating information. (Source #003)

OGC response: OGC agrees. (Source #003)

[edit] (TS//SI//REL) Targeting foreign 'members' of a group

Is it okay to target the foreign actors of a loosely coupled group of hackers...such as with Anonymous? For instance, Anonymous has a 'branch' in Brazil, India, Germany, etc. Can we target those individuals?

NOC/OGC RESPONSE: As long as they are foreign individuals outside of the US and do not hold dual citizenship...then you are okay. (Source #001)

[edit] (TS//SI//REL) Malicious foreign actor == disseminator of US data?

Can we treat a foreign server who stores, or potentially disseminates leaked or stolen US data on it's server as a 'malicious foreign actor' for the purpose of targeting with no defeats? Examples: WikiLeaks, thepiratebay.org, etc.

NOC/OGC RESPONSE: Let us get back to you. (Source #001)

[edit] (TS//SI//REL) Storing 'leaked' US data on government systems

Can we store leaked information (such as from the hacker group Anonymous) on government systems for the purpose of analyzing the data for clues as to the method of the breach?

NOC/OGC RESPONSE: If it's DOD/.mil (and not classified data), it's okay. otherwise no. (Source #001)

NEED FOLLOW-UP: what about .gov data???

[edit] (TS//SI//REL) Querying on foreign IPs obtained from home

If we run across foreign malicious actors at home (spam email, router/IDS logs, torrent sites, etc) can we bring those IPs here and use the SIGINT system to monitor these guys?

NOC/OGC RESPONSE: It might be okay, but wait for confirmation. (Source #001)

[edit] (TS//SI//REL) Foreign servers in which US persons 'might' be using

Is it okay to query against a foreign server known to be malicious even if there is a possibility that US persons could be using it as well? Example, thepiratebay.org.

NOC/OGC RESPONSE: Okay to go after foreign servers which US people use also (with no defeats). But try to minimize to 'post' only for example to filter out non-pertinent information. (Source #001)

[edit] (TS//SI//REL) US server being used for foreign malware call-back

In some instances, foreign malware has a know US server as it's call-back. If we are fairly confident that the URI pointing to the said US server is operated by a foreign actor, can we query for that traffic?

NOC/OGC RESPONSE: If you are more than 50% confident that it is foreign origin, OKAY. Also minimize any potential US legit comms. Also use URI as selector, not IP as server may host multiple domains (some of which could be US domains). If you discover that you are wrong in lessor of said server, then it must be submitted and go into OGC's quarterly report. (Source #001)

[edit] (TS//SI//REL) Tracking foreign actors bouncing through US proxies

[when an actor is]...posting to thepiratebay.org (a foreign web server)...through multiple proxied hops, are we allowed to back-trace that communication even if it hops through US based proxies? In other words, back-trace the post from thepiratebay.org to a Chinese base proxy which came through a US based proxy, which came through another US based proxy, which came through a Russian based proxy, etc.

NOC RESPONSE: Assuming you mean via SIGINT metadata, then SPCMA-trained analysts would be able to use SPCMA-enabled tools to chain through the U.S. based proxies. It is not authorized otherwise. See: [redacted]. (Source #003)
URL redacted

OGC RESPONSE: OGC agrees with the above discussion regarding metadata. (Source #003)

NOTE: V252 has now been given the authority to gain SPCMA access/tools. Analyst should obtain SPCMA training and download the appropriate SPCMA enabled tool in order to achieve the goal in the question stated above. [PUT LINK TO PAGE HERE]

Can we task XKS-SIGINT for communication between 2 US IP addresses if we know the ports associated with a proxy running between them being used for malicious foreign activity?

NOC RESPONSE: If you know the ports associated with the proxy you're targeting are only used for that purpose, then you can target the IP addresses "and" the ports to only return the malicious foreign activity being conducted via those IP addresses. (Source #003)

OGC RESPONSE: However, OGC will need further clarification before signing off on targeting 2 US IP addresses. (Source #003)

Since we can do the above, what level of effort and justification would we provide to filter out US communication? Could we simply use a 4-tuple (the two US IP address on either end along with the port numbers that the proxy is running over) with a justification that it was being used by a foreign power at that moment in time?

NOC RESPONSE: If the 4-tuple task already effectively limits the collection to the foreign intelligence target, than yes. But if your tasking could also result in domestic collection (U.S. to U.S.), then additional defeats or tasking parameters are necessary, perhaps adding a time frame to limit collection to "that moment in time" when you expect the activity to occur. (Source #003)

OGC RESPONSE: OGC agrees and defers to SV regarding the specific filtering requirements. (Source #003)

[edit] (TS//SI//REL) Password == US person?

Does a password correspond to a US person. [If a] list of .mil passwords [were] released to thepiratebay.org...can we go back into XKS-SIGINT (using a custom created fingerprint) to search for traffic containing that password in foreign traffic just before the release?

NOC RESPONSE: Normally a password would not be considered equivalent to a U.S. person, since it is not necessarily unique to any one individual, but in this case, we will have an equivalency record (as will the public!), so I am not sure of the legality from that standpoint. But more importantly, the tasking of the passwords in this case is consistent with the SIGINT Consensual Collection package signed by Cmdr, USCYBERCOM and DIRNSA, appropriate to both of his hats. Refer to this document for full context: [redacted]. (Source #003)

OGC RESPONSE: OGC agrees. (Source #003) URL redacted

[edit] (TS//SI//REL) Botnet on US box, foreign actor

If we have evidence that malicious activity is originating from an US IP via a foreign controlled botnet, can we target that IP using the botnets port number (thus filtering out any US citizen communication)?

NOC RESPONSE: Yes, you would only be collecting the foreign target's use of the U.S. IP in this case, with the appropriate filters ("ands"). (Source #003)

OGC RESPONSE: Again, it is critical that foreignness is established and that there is effective filtering. (Source #003)

[edit] (TS//SI//REL) Definition of Malicious Activity

In reference to the many queastions above, please define 'malicious activity'. Malware server, C&C node, responsible for attacks against a US system, a site containing US persons passwords and other confidential data, a site containing .mil passwords/data, etc?

NOC RESPONSE: The DJP-maintained Cyber Lexicon does not define "malicious activity", so will have to table that for now. But the activity you've described clearly constitutes a security threat to National Security Systems.

OGC RESPONSE: OGC agrees.

[edit] (S//SI//REL) Using SIGINT system for defensive means?

Example: Can we query XKS-SIGINT using a DOD IP address as the selector to look for foreign targets?

Unanswered at this point.

[edit] (S//SI//REL) SPCMA: Query against US selector

(S//SI//REL) When querying with a SPCMA enabled tool (i.e. Synapse Workbench) against a US selector (i.e. an IP address), what are some scenarios that would be considered "Foreign Intelligence purposes"? Based upon the link [redacted], we can query the said US selector "regardless of the known or unknown foreignness of the communicants". Is this a scenario where we are able to query/chain through comms, but must simply de-task if it is revealed to be US origin? URL redacted

(S//SI//REL) EXAMPLE: We have an US IP hitting the NIPRNet with an attack. That attack could very well have a foreign actor behind it, utilizing that US box as a last hop. But it could just as easily be a US person hitting us...we have no idea. Can we assume it is a foreign actor until we have evidence to the contrary? If chaining back through the link (utilizing a SPCMA tool) reveals a US source (as opposed to foreign), do we simply de-task, or would that incidental targeting of a US person need to be reported to you guys as well?

NOC RESPONSE: (S//SI//REL) If SPCMA analysis reveals a U.S. actor behind an intrusion, then per SPCMA guidance "Existing rules for collection and dissemination of US person information are unchanged by the Supplemental Procedures." Therefore, you would de-task the U.S. actor (if previously tasked vs. incidentally discovered), and this would be a reportable incident. However, if not previously tasked, the discovery of this U.S. Person would be incidental to a legitimate foreign intelligence task and therefore discovery via authorized SPCMA chaining is not an incident. (Source #005)

[edit] (TS//SI//REL) Querying on Case Notation

XKS-SIGINT queries being made with a 'case notation' as the selector. There are two scenarios...

1) An XKS query being made with only one or more case notations and a time range (typically in days and always exceeding 2 hours) being used as selectors.

2) A query being made with a case notation selector AND a minimal amount of effort to narrow down the query...such as looking for executables only – see example #2 below.

In neither case, are there any sort of FVEYs defeats, timeframe limitations (such as a 2 hour window), nor 'malicious' fingerprints being used. And in case it matters...these are typically Cyberquest personal at remote field sites whose tasking includes survey work such as characterizing links for possible SIGINT value. If BLACKPEARL shows the case notation/link to be foreign (Saudi Arabia, Denmark, etc.) is that justification enough to query on that case notation alone with no other defeats?

NOC RESPONSE: For the purpose of characterization activity, the queries are supportable, given the confirmation from BLACKPEARL that the case notations are foreign. A case notation is also considered a strong selector and any additional limiters would be more to restrict the volume of the return than anything else. Although not recommended for sustained collection, but are fine for survey purposes; consistent with the mission being worked by the Cyberquest personnel. (Source #004)

[edit] (UD//FOUO) Other guidance to review

If your answer is not on this page try this OGC roundtable link

[edit] (TS//SI//REL) Sources

Source #001 Analytic round-table on 25-JUL-2011 @ 0930 with: [redacted] D NSA-V07 USA CIV; [redacted] J NSA-V222 USA CIV; [redacted] R NSA-D21 USA CIV; [redacted] M NSA-D24 USA CIV; [redacted] T NSA-V222 USA CIV; [redacted] M NSA-V07 USA CIV; [redacted] M NSA-V07 USA CIV; [redacted] D NSA-V225 USA CIV; [redacted] NSA-V3 USA CIV; [redacted] P NSA-V222 USA CTR

Source #002 Email from: [redacted] T NSA-V222 USA CIV (U) change in auditing policy 6/15/2011 media:Change_in_auditing_policy.doc

Source #003 Email from: [redacted] D NSA-V07 USA CIV (U) FW: (U) USSID18 questions from a V252 analyst Friday, June 24, 2011 10:29 media:USSID18_questions_from_a_V252_analyst.doc

Source #004 Email from: [redacted] F NSA-V07 USA CIV RE: (U) Question about querying on Case Notations Wed 8/24/2011 12:02 media:Question_about_querying_on_Case_Notations.doc

Source #005 Email from: [redacted] M NSA-V07 USA CIV, RE: (U) QUESTION: SPCMA clarification, Wednesday, August 31, 2011 4:46 PM media:QUESTION_SPCMA_clarification.doc

NSA employee names redacted

TOP SECRET//SI//REL TO USA, FVEY
Derived From: SI Classification Guide, 02-01, **Dated:** 20060711
and NSA/CSSM 1-52, **Dated:** 20070108
Declassify On: 20320108

Derived From: SI Classification Guide, 02-01, **Dated:** 20060711
and NSA/CSSM 1-52, **Dated:** 20070108
Declassify On: 20320108
TOP SECRET//SI//REL TO USA, FVEY