Summary of the April, 2010 DNS-CERT Operational Requirements and Collaboration Analysis Workshop

Spring, 2010

Report authors:

Jose Nazario, Arbor Networks

Roy Arends, Nominet

Chris Morrow, Google

Executive Overview and Summary

On April 6 and 7, 2010, ICANN hosted a tabletop exercise in Washington, D.C., USA, to review Internet and DNS security scenarios. The 21 Participants included five members of ICANN staff, one DNS vendor, two gTLD registries, four ccTLDs registries, one registrar, security staff of Google and Microsoft, various DNS security and research organizations, and operational security community individuals. The purpose of the exercise was to discuss various scenarios, and identify how the members of the community around the table presently respond to an array of Internet and DNS security threats, such as malicious names, malware using DNS, denial of service attacks, and security issues involving domain names, registry and registrar operations.

Participants identified several requirements for responding to Internet and DNS security events, many of which are under-met or ignored by existing DNS security capabilities. They are:

- A trusted communications channel, or multiple channels, for use during event response that is usable by the appropriate parties.
- Standing incident coordination and response functions, which enable consistent and professional incident handling efforts.
- Incident status tracking through to completion, with communication to the necessary partues.
- Trusted guidance on issues with knowledge and experience with the various and varied areas of Internet and DNS security. Respect of these voices by the areas of the Internet and DNS communities with which they speak is important.
- A trust broker / introduction service across traditional communities boundaries, recognizing that the community identifying threats to Internet and DNS operations is often far-flung and sometimes outside the knowledge of the Internet and DNS operator and vendor communities.
- Analysis capabilities, including data such as DNS traffic, software vulnerabilities and attack traffic, to validate incidents and identify next steps as quickly as possible.
- Institutional memory in the form of reports, recommendations, and best practices, which can inform the various Internet and DNS security communities, support future successful incident responses, and help evolve incident response capabilities.
- Outreach and education functions to share best practices for securing Internet and DNS operations, secure registration functions, implementing DNSSEC, and other key DNS and security factors.
- The ability to act quickly, and to be prepared to act with necessary resources in response to threats to the DNS of a global nature in a timely and sustained manner.
- A sensitivity to the complexity of the international nature of the DNS, understanding the capabilities and limitations of the global DNS community.

Workshop participants noted many of these functions are addressed by various groups, either standing or ad-hoc. Some participants expressed concern that only a few of the existing organizations are DNS-specific.

Notes:

Participants noted some of the great challenges associated with improving security on such a large, multi-stakeholder system like the Internet, and did not delve into whether or which of those challenges are solveable.

The workshop expressly did not consider the possible budgets of any future DNS security efforts or how they would be financed.

The views expressed by the workshop participants do not necessarily reflect the official positions of their employers.

The scenarios were distributed just prior to the meeting, thus making it discussion of the individual participants' views and experiences.

Some workshop participants will include detailed comments under separate cover.

Event Overview

The tabletop exercise event was organized by ICANN staff members. Invitations were sent to the DNS, security policy, and the security operational and vendor community that have participated in recent, global DNS security efforts. These participants are specially positioned to both review DNS-specific security responses as well as general Internet security response capabilities.

The majority of the exercise was conducted through scenario analysis. ICANN staff prepared scenarios that represented previously seen issues affecting global DNS stability and security scenarios, and participants were asked to consider the following questions:

- What would the community of DNS, security, and networking professionals do?
- What would your organization do?
- What role could a DNS-CERT function play?
- Who is not engaged by the present situation?

The goals of the scenarios and these questions were to analyze the current response functions and to identify the requirements for anyone offering Internet and DNS security support services.

Participants represented a wide variety of groups, including ICANN, registrars and registries, DNS services and software infrastructure vendors, DNS security groups, security researchers, and some members of the Internet security community. Some of the groups present already provide some of the functions required to respond to the scenarios. This capability overlap was intentional. A full list of participants is given at the end of this document.

Scenario Analysis Review

The following scenarios were provided by ICANN staff prior to the workshop to the participants. Not all proposed scenarios were addressed.

Scenario 1.1

The first part of the first scenario focused on a global response to a scenario that has occurred in the past and may occur again:

Klingon is an opensource software package that is used by smaller registries as an "all in one" solution. It gives them everything that is needed from the interaction with the registrars through to the publication of the zone.

Recently a bug has been discovered in code that controls the way that EPP transactions occur between the registrar and the registry. The bug allows for unauthorized changes to registrations to take place. Currently there is no indication that malicious actors have used the bug in the wild.

As this software is free and unregistered the author has not been able to determine which registries are currently using the software. A patch is in the process of being developed. It is estimated that as many as 30 TLDs and their registrars could be affected.

Workshop participants described that the current community of DNS, security, and networking professionals would respond as follows: Identify what the nature of the vulnerability is, identify who to contact to address the bug in the software, and then identify who to contact directly to ensure that it is patched in deployments quickly. The consensus of the registrars and registries at the workshop was that they would work through the software vendors, and probably with little publicity, to request and deploy the security patches. Registries/registrars noted that this process places the vendor at the center of assured communication with its customers (those needing the patch), status tracking, an authoritative voice for validation and a trusted and known vulnerability coordinator. Some participants noted that in certain cases, such as when exploits are actively in use, someone familiar with the software may create and circulate a patch for open source software packets to known users as a stopgap measure. Participants also noted that the response may depend on who identified the bug; for example, the vulnerability discoverer may not always know which communities are affected and may not have contacts in all affected communities and may choose to publish the bug openly, for example on a vulnerability disclosure mailing list such as Bugtraq, placing the community at risk. Registry operators present noted that they would not work with a software package that was unmaintained and where they did not have good communications with the author. Participants generally agreed that the risk severity of the bug would dictate the speed and intensity of the response.

Exercise participants agreed that having the ability to notify all users of the software vulnerability, to validate that the software is properly fixed, and to work with users to ensure that it gets upgraded properly, is a key requirement for anyone performing DNS security services in this scenario. Some noted that this is already a critical factor of their work.

Scenario 1.2

The second part of scenario 1 focused on a global DNS operational bug, similar to the August 2008 Kaminsky bug:

A new bug has been has been found in a major brand of DNS resolver code. The bug allows for easy poisoning of the cache. The code is in use by many ISPs and businesses throughout the globe. As it is an issue with cache poisoning it does not affect authoritative only name servers.

The participants noted that many of the same efforts would be needed in this scenario as in the previous scenario, that is bringing together the vulnerability discoverer and the software vendor, ensuring the vulnerability is mitigated, and that the affected parties can deploy updated software. However, the scope of distributing the software patch, hotfix or workaround involves multiple parties, some of which are not usually part of the DNS operations community. These include OS Independent Software Vendors and other vendors who may ship this software to their customers, ISPs who have deployed the software at customer-facing DNS servers, and customers who operate on premises resolvers. This is similar to other OEM software with a broad userbase, such as HTTP server software, operating system kernels such as Linux, or TCP/IP protocol stacks where major bugs have been found. Participants noted that depending on the bug and whether exploit code is known to exist, they may monitor major DNS servers for signs of attacks in an attempt to poison DNS caches, affecting end-user security.

Some participants noted that the handling of the Kaminsky bug did feature trusted communications, and an authoritative vulnerability coordination role.

Some participants identified the following requirements for these two scenarios:

- Complete, reliable and trusted communications of the issue between the discoverer of the vulnerability, the software vendor, and operators and users (in certain circumstances, these communications may be sufficiently sensitive to merit confidentiality measures such as encryption).
- Status tracking, to ensure that the issue is resolved quickly and at the key user points.
- A trusted voice that understands the DNS security and services community who can validate the issue and its resolution.
- Vulnerability coordination role, involving the right people are involved at the right times .
- Trusted broker between vendors, vulnerability researchers, and users, providing introductions or acting as a message conduit between the parties. This broker must be trusted by all of the parties involved.
- A contact list of who provided the software and fixes, and who are the major sites (e.g. ISPs) using the software, to ensure that it is fixed quickly and in major deployments.

Scenario 2.1

The second scenario focused on security events that affect registries that do not routinely communicate with the security community. The first part of the scenario focused on active exploitation of a backend registry system shared by multiple ccTLDs:

Hackers competition site reported DNS records associated with .id, .kh, .vn, .ml, .ug domains were hijacked by hacker name RED.

According to this site, RED targeted ccTLD operators registration package system "Doremi", based on a PHP and MySQL backend, obtained the user logins and passwords for a number of high profile domain names including Google, Microsoft, Citibank and others, by using SQL injection method, obtained privileged access to "Doremi" commonly used among small registrars.

RED used the domain name credentials to modify the DNS configuration of domains and re-direct them to the defaced site, which is distributing malware, hosted in Russia.

Participants noted that the corporate organizations affected may likely involve legal action and seek court order level actions in the process to protect their corporate identities. Participants who were TLD operators noted that they would be able to review the changes and revert any suspicious changes. All participants, including registry and corporate participants, agreed that the key steps would be to identify how much damage was done, revert the changes, and prevent future breaches by working with the software vendor to find and fix the issue. Participants from the ISP security community stated that in such situations it works to take down the malcode site, as well, and possibly get logs showing the number of affected clients. ICANN has, in the past, worked to notify other registry operators using vulnerable software to ensure fixes get installed as soon as possible.

Scenario 2.2

The second part of scenario 2 focused on a very common event, where a security researcher is unable to communicate an abusive domain name to the registrar, who (in this scenario) publishes contact information but not security contact information, has not responded:

Security Company name Cyber Cop reported NXDomains list, domain names used only for distributing malware.

Cyber Cop requesting for responsible registrar "Dalmatian.biz" to suspend the domains, but Dalmatian.biz publishes no contact information for security response, and no response back.

Workshop participants noted that the specific scenario involves a well known and connected TLD operator, and that the process invoked is to escalate it to the registry and let them work the issue with the registrar as needed.

After discussion, participants identified the following requirements for this scenario:

- A trusted voice who can provide clear, experienced guidance for this incident for all parties involved. Some parties, such as researchers who discover domain name abuse, are outside of the normal DNS operator community. Some DNS operators may not know who to trust with security complaints and need to turn to a trusted third party. Furthermore, some registries may need assistance to identify suspicious registrations and changes to existing registrations.
- Validation and verification of the incident, that the domain name is indeed being used for malice and that it's suspension would be safe, which requires analysis experience and data.
- International coordination for the issues, and sharing status updates with the community, including the researchers who discovered it and the DNS community at large.
- Awareness raising to registries and registrars about such security incidents and the best practices in their handling, specifically around investigating malicious domain name use and how to response to such incidents.
- Interfacing with law enforcement as needed for any investigations.

Some participants stated that timeliness is a key factor for these scenarios, something that is sometimes delivered, but not ensured by the current ad-hoc response system. Also the current security response system, made up of mostly volunteers, often fails to provide adequate communication to the necessary parties.

Scenario 3.1

This scenario looked at availability attacks on the DNS infrastructure. The first part deals with a DNS DDoS attack on an operator that hosts zone files for multiple TLDs:

Empiricus Registry provides global backend registry services for 5 ccTLDs and 8 gTLDs. Empiricus has its headquarters in Tiberium, Mediterranea (formerly headquartered in Londinium but moved due to tax benefits within the EU) with NOCs in Londinium and Seattle, Washington, with secondary site in Cologne, Germany. Empiricus services 30 million domain names worldwide.

Empiricus has multiple data centers, supports thick and thin registries, and complete support for IDNs.

Empiricus announces that it has won a contract to provide backend registry services for a Soranji IDN TLD using the Arabic script (Soranji is a fictional language spoken by 20 million people across parts of Central Asia, Europe and the Middle East).

At time point (xx:xxhr) the registry starts to see large amounts of traffic to the published NameServers.

Packet streams are in excess of their Bandwidth capacity.

Upon inspection of the packets they appear to be UDP DNS queries, with 100 unique *source IP's and 50 differing queries.*

Upon further investigation the IP addresses are from 100 well-known ISP recursive nameservers, queries are for 50 well-known banking websites.

Workshop participants expressed that the first action would be for Empiricus to reach out to the immediate upstream ISPs for the Empiricus name servers to investigate traffic filtering options. This action should be treated as a normal course of business Denial-of-Service attack by the victim. Normal incident response procedures should be used by the registry to mitigate an attack such as this.

Scenario 3.2

The second part of the scenario looked at an availability attack on the registrar's web front end, which would affect domain management for all external users:

A large DDoS is initiated against multiple registrars their web sites are the target and are no longer able to respond. This means that they can neither sell new names nor accept updates to existing customers names.

All indications are that this is a large botnet, source IP addresses seem random and the HTTP gets look valid. The bandwidth usage is massive; pipes at server farms are fully utilized.

Workshop participants noted that measures to respond to a security event of this kind should be part of customary security practices for operators in the registrar or registry business, but may not be common. Detection and countermeasures approaches include blocking access from some geographic regions during the peak of the attack, HTTP request rate limiting through deep packet analysis, and client IP blocking. The goals of these tactics is to keep as much of the legitimate service running for as many users as possible. These existing relationships with upstream providers or other registrars could be leveraged in mitigation and information sharing efforts. Upstream ISPs provide the bandwidth capacity, and often the expertise and equipment, to address such attacks. Also, other registrars may suffer the same kinds of attacks on their infrastructure and should be aware of this attack threat to protect their users.

Based on these scenarios, some workshop participants identified the following key requirements to address such a scenario:

- Attack information sharing and trust validation of the parties involved in resolving the incident, between the operators, analysts, and ISPs. Not all DNS registrars have the needed communication paths to their ISPs or the capacity to analyze such events and seek remediation.
- Secure communications channels between the parties involved in the incident response to ensure confidentiality and authorization.

- Analysis of the traffic to determine countermeasures or next steps. DDoS attack analysis skills are crucial in these situations to both stop the attack and to preserve as much legitimate traffic as possible.
- Preparation and capacity planning for such scenarios for registries and registrars to address the threat of such attacks prior to their occurance.
- Possible law enforcement interactions when needed.

Some participants noted that detection and mitigation systems for DDOS attacks are already widely in place, part of the security planning of the registry service providers, and part of plans offered to registries by Neustar and Verisign, among others.

Scenario 4

The fourth scenario the workshop addressed is of a domain generation algorithm present in malcode, similar to the Conficker incident:

During routine analysis of code taken from an infected machine a piece of code that generates domain names is discovered. The code is part of an update that was sent to via the command and control mechanism of a large and growing botnet (numbers in the millions).

The code generates 50000 domain names in 200 TLDs each day. Although the strings appear random they can be pre-generated.

It appears that the infected machine will pick 50 randomize strings from the 50000 and try to contact. Each day it will pick 50 from the new batch of 50000.

Those investigating the botnet have gathered intelligence that lead them to believe that the infected machines could be bought into use in the next 48hrs to launch a major DDoS attack.

Their suggested mitigation is the blocking of registration of names.

Workshop participants described how the Conficker response effort was undertaken, but it was stressed that Conficker was an exceptional situational response effort that would not be easily reproduced. Conficker was contained by an ad-hoc, all volunteer force that had more time to contact necessary TLD operators than the above scenario gives. While ICANN assisted in establishing communications channels between the security and DNS communities (and particurly with TLD operators), participants noted that even ICANN's contact list was found to be incomplete. The anti-malcode researchers were hard pressed to to determine and distribute the daily list of algorithmically generated DNS names Conficker would use. TLD outreach was a key action (in this case facilitated through ICANN). Monitoring efforts were largely lead by the community or anti-virus companies. TLD operators noted that a key element in the case of Conficker was ensuring the of the list of domains, and that having the list be delivered with adequate time to investigate and, in some situations, to seek the necessary legal paperwork to block domain use was of paramount importance

Some participants distilled the following requirements from this scenario:

- A secure communications channel, ensuring confidentiality and authorization between researchers, ccTLD operators, and others needed to provide support in this response.
- A complete and accurate contact list of the ccTLD operators needed for the response.
- An analytic capacity our access to such capacities, specifically to reverse engineer and analyze the domain generation algorithm.
- An incident management role to ensure that the participants in the response are working in concert and
- Trusted guidance to TLD operators about how to respond to this scenario, such as how to block domain name registrations and for how long.
- An understanding of TLD policies within specific TLDs, where some are not allowed to block domain name registrations without legal orders.
- An incident historian to capture and record the lessons learned as they occurred for future reference.
- Resources to work with registries without the capacity to block domains on this scale and for this duration to analyze existing registration collisions for possible attacks by the malcode author and to verify the list of domain names.
- Preparatory planning and exercising, which will test the ccTLD contact list and verify their ability to respond to such scenarios.

Scenario 5.1

This scenario dealt with a DNSSec Key Compromise/Failure at a fictional TLD, .dog:

During investigations by (law enforcement) of suspected malicious DNS use a strange behavior was discovered. Despite the use of DNSsec it appears the some specific domains within the TLD .DOG are returning incorrect NS records. However these records appear to be validating.

All indication is that a version of the .DOG zone is being used by a third party. The DS records for bigco.dog have been changed and the .DOG zone appears to have been signed with a valid ZSK.

Initial analysis would suggest that the malicious actor has been able to obtain (or generate) a valid ZSK for .DOG.

It is not yet clear what the mechanism for injecting these answers is but customers of multiple large ISPs have seen them.

Participants made it clear that when this happens one of two things could have happened. Either the private .DOG DNSKEY has been leaked, so a malicious actor is able to sign alternative data, or a malicious actor has access to the database and is able to change records before they are signed. Either way the .DOG procedures are considered broken. The obvious route is to identify the broken procedure and fix it. Additionally, the operator must roll its key. For TLDs, the obvious way to roll the key is to talk to IANA and introduce a new DS for .DOG in the root zone. Additional measures to mitigate the amount of bad data are to track the most popularly used DNS resolvers, contact their operators and ask them to flush their caches to quickly affect the greatest number of users. Auditable procedures, proper roles and educated actors are essential to a successful and safe DNSSEC deployment and maintenance. To limit the amount of reputation damage and rebuild the publics trust in this scenario, transparency and public third party audits are important.

After discussion, some participants identified the following requirements to address such a scenario:

- A contact list of necessary parties to rapidly address the problem, including key managers, DNS root and TLD operators, ISPs, and major caching resolver operators.
- A list of best practices around DNSSec key management, access controls, and industry strategies with similar security needs to identify when a key compromise has occurred, to prevent such a compromise in the first place, and to ensure that the right representatives in key management are identified.
- A government liaison (for ccTLD operators affected, which may affect government operations online) and a trusted, verified information source to provide accurate information to the parties needed to revoke the key and discontinue its use.
- A coordinator across the different groups who are responding to the issue across government,

Other Scenarios

Scenario 5.2, 6.1 and 6.2 were not discussed due to time constraints.

Distilled Requirements and Current Community Efforts

The requirements gathered from the scenario analysis summarized above produced ten findings that were common to many of the scenarios. The final session of the workshop took the findings and identified which are met, partially or completely, by current registry, registrar, Internet, vendor and/or community efforts. Current responders include commercial vendors, established organizations such DNS-OARC, RISG, the Conficker Working Group (CWG), FIRST, various CERTs around the world, and academic/vendor/registration ad-hoc communities such as trusted, operational mailing lists.

Workshop participants identified groups and communities that both directly focus on the DNS security community and also broader operational security issues on the

Internet that affect the DNS.

Requirement 1: Trusted communications channel, ensuring message confidentiality, authentication, and integrity; a complement to trusted channels is a comprehensive contact list for DNS security.

Participants agreed that operational DNS security relies on trusted communications channels that all parties can trust. This requirement is partially met by the following groups:

- RISG, who has good contacts in the registry and registrar community leadership from security community and focuses on identity theft and malware.
- DNS-OARC, where a number of registries and registrars are members and other members are from academia, the security community, and key vendors and offers a secure communications system.
- SSAC and RSSAC mailing lists, which are more strategic than operational.
- Numerous security operations community mailing lists (e.g. Ops-Trust) which provide considerable trusted communications and information among and interaction between problem finders, vendors and the security community. Some provide encryption for the mailing list, although this functionality is not commonly available in all operational security communities. Some noted that these security operations communities are fragmented and typically invitiation only, meaning they reach only a small subset of needed parties.

Participants agreed that while trusted communications are partially met by these groups, in terms of membership covering DNS security and coverage across DNS security incidents, no single list has comprehensive participation and the communications are largely not coordinated at present.

Requirement 2: Issue status tracking, an organization who works to ensure that an issue is resolved to the satisfaction of the parties involved.

While this requirement is partially met by DNS-OARC for some specific events, such as it did for the Kaminsky attack vector of 2008, DNS-OARC is staffed nor funded to operate as a global tracking center or tracking coordinator/facilitator for many security events. Some participants thought that the number and diversity of incidents that should be treated with the kind of tracking DNS-OARC performs exceeds DNS-OARC's capacity.

Requirement 3: Trusted guidance in the Internet, DNS and security communities, whom parties trust providing timely and accurate information.

The DNS security community often looks to ICANN, ISC, and DNS-OARC to meet this requirement. CERTs and vendors partly fill this role for the DNS security community.

Participants, specifically parties from ICANN, noted that ICANN is often regarded by people outside of its direct sphere of interaction as the first, best point of contact for any DNS issues. While those within the ICANN community may believe that ICANN is not commonly set up for this role, the broader Internet community will continue to view ICANN as the only identifiable entity that appears to fit the role.

Requirement 4: A trusted communication facilitator, acting as a intermediary or as an introduction service.

This is a complement to Requirement 1 (a trusted communications channel), where groups need a clear facilitator of trusted communications. Such a service may act as a broker introducing parties to resolve an issue, or as a proxy for one or more parties involved in resolving an incident. It was commonly agreed that such a service must be trusted by all parties involved to have value. Workshop participants identified the following groups who currently partially meet these requirements:

- CERTs (national, sector specific) often act as an intermediary service
- Security operations community mailing lists (e.g. NSP-SEC, Ops-Trust, NXDOMAINS) that often act as a trusted introduction service, either on-list or with off-list introductions
- NANOG and other regional ISP network operator groups

Participants generally agreed that while these groups serve their members well, their reach and remit are limited, but noted the plans of these organizations to grow and expand.

Requirement 5: Creating and maintaining institutional memory, and sharing this knowledge in the form of reports.

Historic knowledge and experience was regarded by the participants as vital to ensure incident resolution proceeds smoothly and quickly, and was noted by at least one member as a key factor in building a professional response organization. The group also noted the value of regular or incident-specific reports and post-incident analyses (such as the Conficker after-action report) to propagate insights and best practices to the broader DNS and security operations community. The following groups were identified as providing this service to the DNS community:

- CERTs, who produce open guidance for constituents and the community at large on general Internet security matters
- ICANN and ICANN SSAC, who have produced recommendations around security events

All of the participants agreed that the function of capturing a major event's history as it occurs, analyzing that history, and using that knowledge to improve future incident responses, while important, is very infrequently done. Most of this analysis, when it is done, is done after the event has concluded and is made from recollections and possibly from mailing list archives.

Requirement 6: Analysis capabilities, assessment and escalation functions.

Participants agreed that some analysis capabilities are required for any group providing DNS security support to assess, verify and escalate issues appropriately. However, participants also agreed that these capabiloities should augment but not duplicate existing efforts available in the community, presently performed by:

- CERTs, who have in-house analysis teams and also close collaborators
- Vendors, who have in-house analysis teams for software or protocol vulnerabilities
- Universities and research organizations
- Other private sector players (for profit players such as brand protection companies, NFP anti-* orgs, LE supporting agencies such as NCFTA...)

It was generally agreed by the participants that analysis capabilities by such a DNS security group could be "thin," meaning partly met by a central group but often drawn on from external parties as needed, such as anti-virus researchers and vendors, anti-spam or anti-phishing communities, software vulnerability experts, or the like. Participants noted that the kinds of analysis required are so broad and often met by existing groups within the DNS community and outside of it that it does not make sense for any DNS security provider to attempt to staff deeply for all threat topics but instead work with existing teams when possible. Existing groups provide and will provide considerable analysis capabilities.

Requirement 7: Community outreach and education functions.

Participants noted the valued function of CERT teams is to collect incident data and insights, as well as lessons learned, and to produce after action reports for major events or to distill these findings into best practices collections. These resources can be drawn upon by the community for education purposes or guidelines for implementations. Furthermore, CERT organizations dedicate efforts and resources to establishing contacts to all elements of the security response community, such as security researchers, ISPs, operators, registries and registrars, and vendors. This gives them a large, trusted contact list and places them inside a circle of trust for needed parties as incidents arise.

Participants note that at present the following groups fulfill this role generally or for the DNS security community, or they look to these groups for such guidance and contact information, and agreed that these organizations provide decent coverage that could be expanded.

- ICANN
- CERT organizations and FIRST
- Internet Society
- ISC
- NANOG/JPNOG/SANOG/etc
- MAAWG
- ISC and other vendors
- APWG

Note that some of these groups are not specific to DNS, and some organizations are membership based.

Requirement 8: Incident response coordinator across various parties such as researchers, registries and registrars, vendors, and operators.

Workshop participants recognized that the scenarios used highlight the broad number of individuals who work to identify abuses of the DNS, such as fast flux, infrastructure attacks, and vulnerabilities in DNS management tools. Not all of these researchers who discover DNS security issues necessarily know who to contact and what information to provide. While there are groups that work in this area, they are not accessible or known to all necessary parties. At present, the community sees the following major groups working in this area:

- CERTs
- DNS-OARC
- Operational security communities (such as NSP-SEC, Ops-Trust, NXDOMAINS)

Requirement 9: Capacity to ensure a timely response with some frequency, and to sustain that response.

While workshop participants described that they could address many DNS security responses with their existing social and professional networks, they largely acknowledge that the speed with which remediation can take place varies greatly depending on the action needed and the ability to contact needed parties. For several scenarios reviewed, timeliness was recognized as a critical requirement to contain the damage being done to the global DNS. Furthermore, the Conficker response raised the concern about the frequency with which broad efforts can be mustered with a largely volunteer force who are not focused on DNS community security response. Participants hailed the Conficker Working Group and its creation, but also recognized that such efforts are not sustainable for the long term, nor are they reproducible.

Workshop participants agreed that they seek the assistance from the following groups for such matters and feel that the response timeliness is adequately met for many issues, although this is not a DNS-specific community:

- Global CERT organizations, who have a standing, professional staff with resources and training to handle security incident response requests from their communities.

Participants agreed that in the DNS-specific security community, this response capacty and base of knowledge is presently uneven and lacking across the broad range of issues. Documentation exists on secure DNS architectures and configuration guidelines, DNSSC deployment guidelines, and secure DNS guidelines for ISPs, DNS operators, registries and registrars but is not centrally collected. Furthermore, very few groups are focused on developing new material in this realm.

Requirement 10: Sensitivity to the complexity of an international coordination role, as well as the ability to act internationally.

The workshop highlighted the international nature of the DNS. With ccTLDs, for instance, multiple nations' governments may be affected. Requirements for addressing issues varies by country, with some requiring a court order to suspend a domain name. Any global DNS-security effort working with multiple nations must be aware of these hurdles. Furthermore, language barriers, budgets, and capabilities vary widely across the world, again requiring an understanding to deliver assistance.

Workshop participants identified the following groups with demonstrated experiences with handling such issues.

- ICANN
- PCH
- DNS-OARC
- CERTs, FIRST

DNS Security Response Gaps

Analyzing the scenarios from the workshop and the common requirements from the previous section, gaps in present Internet and DNS security community capabilities begin to emerge. As noted above, some of the requirements are partly met by existing groups. Their coverage in these areas, however, is uneven, leaving many DNS stakeholders unserved or under-served; DNS security issues cannot reliably be addressed for all parties quickly and throughly. In short, Internet and DNS security may require a reliable, well known and trusted body for all parties to utilize to address Internet and DNS security incidents, something which is not met at present.

The largest gap in the requirements participants identified in the existing Internet and DNS security community is timeliness and the capacity to respond to events with a potential global impact reliably and consistently. Because so much of the existing DNS security community is volunteer-based, primary employment requirements often take precedent over community response efforts, as happened in the Conficker response. While CERT organizations exist in much of the world, they are often disjoint from the DNS and registry operator and security community, making communication across these traditional scope boundaries difficult.

Another large requirement some felt that is very poorly met in the DNS security community presently is a trusted intermediary or introduction service, which itself has the requirements of an extensive DNS, security, threat researcher, operations and vendor contact list, and also requires trusted communications channels usable by these parties. Many of the incidents analyzed required these facilities to remedy the security incident; without them, problems may linger or resolve slowly. Currently the DNS security community uses the membership-based organizations DNS-OARC and RISG, each of which have some globally small portion of the DNS security community involved, meaning their reach is limited. Their membership models also produces a barrier to participation for some, hindering these organizations' growth. Other workshop participants noted that fee-based membership models likely produce a disparity between those who receive response services and those who do not, limiting such an organization's effectiveness to truly operate globally.

Security operations lists, such as NSP-SEC and NXDOMAINS, provide their members the ability to make contacts at distant organizations during security incidents. However, they have limited reach, globally, and fail to include many major and minor stakeholders, such as registries, registrars, TLD operators, and ISPs. Furthermore, their access is gated by design to trusted individuals through an invitation and vetting function vital to their operational security, meaning a person normally outside of the community cannot utilize those resources; these lists and communities must grow via their existing social networks, a time consuming process. The result is that these lists serve their specific communities well, but not the DNS security community at large.

Incident management and coordination of DNS security issues in its present form is usually left to either the incident reporter or, in the case of an implementation bug, the vendor once the bug has been accepted into their process. In the absence of good process and experienced management, incident resolution is sometimes delayed or worse, incomplete. Furthermore, the update deployment completeness for only a few major DNS security issues has been measured, including the Kamsinsky attack with DNS-OARC's source port test, and the open recursive resolver measurements by Dagon and Provos. The deployment rates for many more patches for threats to the DNS have largely gone unmeasured.

Addressing this incident management service requires dedicated staff that has performed incident management before, has contact information for the necessary parties, has access to analysis capabilities either in-house or with a trusted partner, has resources to dedicate to ensuring the issue is tracked and brought through to resolution, and is able to communicate needed findings to the community at large afterwards. These communications may take the form of an incident note, a security advisory, or even an after-action report for large incidents, such as the mitigation of the Kaminsky cache poisoning vulnerability or the Conficker malware incident.

Some workshop participants from the operational DNS community also noted that they do not have a single place to get comprehensive, trusted guidance about DNS security or deployment issues, such as guidance on remediating a DNS threat. Multiple sources exist but are not well known or complete. Other workshop participants from the operational DNS community noted that they spend extensive efforts in obtaining and sharing this material. At present no organization reliably offers these services to the whole DNS community. Workshop participants generally concluded that dedicated, full time staff whose primary focus was on DNS security could provide those services to the DNS community, meeting those needs, and do so for a larger portion of the DNS world.

On the whole, workshop participants expressed that while many of them could address the scenarios used in the workshop, they recognized that these facilities are not widely available. The current operational security model, much of which is based around ad-hoc, informal structures, simply lacks the resources dedicated to provide widely available and sustained DNS security efforts.

Workshop Participants

Greg Aaron	Afilias, RISG	Director, Key Account Management and Domain Security at Afilias, chair of ICANN's Registration Abuse Policy Working Group, founding member of the Registry Internet Safety Group.
Richard Wilhelm	Network Solutions	VP of Engineering, ICANN SSAC member
Kathy Kleiman	PIR, RISG	Directory of Policy, PIR
Oscar Robles-Garay	NIC.MX	PIR Advisory Council, member of Latin American and Caribbean Internet Address Registry board of directors
Xiaodong Lee	CNNIC	Vice President and Chief Technology Officer of the China Internet Network Information Center
James Stidham	Packet Clearing House	
Rayman Khan	.GY Registry	Administrator, .gy ccTLD, University of Guyana
Jean-Robert Hountomey	AFNOG	CEO of ISERVICES, member of Diplo Internet Governance Community
Suzanne Woolf	ISC, F-root	Senior Programme Manager for OARC, member of the ICANN Root Server System Advisory Council and ARIN Advisory Council, and member of ICANN SSAC
Karl Hanmore	Microsoft	Microsoft MSRC, previously Operations Manager for AusCERT
Chris Morrow	Google	Network Security Engineer at Google, previously Principal Network Engineer at UUNET/Verizon Business/MCI
Roy Arends	DNS-OARC, Nominet	Director at DNS-OARC, Senior Researcher at Nominet

Keith Mitchell	DNS-OARC, ISC	Programme Manager, DNS-OARC
Jose Nazario	Arbor Networks	Senior Manager of Security Research, head of ASERT, co-founder of Ops-Trust community, involved in CWG
Andre Ludwig	Shadowserver, NXDOMAINS	Founder, NXDOMAINS and OpenSecNet communities, formerly at Neustar, involved in CWG
Dave Dagon	Georgia Institute of Technology	DNS security researcher, previously Senior Technical Advisor to MAAWG.
Greg Rattray	ICANN	Chief Internet Security Advisor, ICANN
Yurie Ito	ICANN	ICANN collaborative response, previously JPCERT technical director, board member at FIRST and APCERT
John Crain	ICANN	Senior Director of Security, Stability and Resiliency, ICANN
Patrick Jones	ICANN	Senior Manager of Continuity & Risk Management, ICANN
Dave Piscitello	ICANN	Senior Security Technologist, ICANN, previously IESG area director

MINORITY STATEMENT

18 May 2010

TO: Dr. Greg Rattray
Chief Internet Security Advisor
Internet Corporation for Assigned Names and Numbers

cc: Jose Nazario
Arbor Networks

RE: "Summary of the April, 2010 DNS-CERT Operational Requirements and Collaboration Analysis Workshop", ICANN table-top exercise

Dear Dr. Rattray:

Thank you for your consideration and engagement on the issue of DNS security, which is of vital importance to us all.

The workshop participants have been given a very short timetable to review the draft report produced by the three co-authors, which does not permit us to perform a detailed review and line editing in collaboration with the authors and other participants. In general, we feel that the workshop, while often illuminating, was also premature in some ways. Also, the draft contains some omissions, needs clearer attribution, and includes conclusions that we do not recall being reached during the course of the workshop. We therefore offer the following general comments, and reserve the opportunity make additional comment in the future. Please include this letter in the report as a minority statement.

The workshop was designed to identify operational requirements and create a gap analysis. By performing gap analysis, the workshop will inform revisions of the DNS-CERT business case. In this ambitious endeavor, the community will want clear statements and substantiation regarding what problems need to be solved, and a proper scoping of those problems. These fundamental scope and mission issues must be better understood before or at the same time that more operational requirements are worked out.

The public comments on ICANN's DNS-CERT Business Case were remarkably in tune with each other, and came from a spectrum of ICANN community members, governments, businesses, and organizations. Most called for community process to examine some high-level issues, including:

- The DNS-CERT's scope and mission are unclear and seem overly broad.
- There is not agreement or documentation regarding the perceived threats to DNS security that a DNS-CERT would be established to address.
- The problem of buy-in and trust from the various stakeholders that own and operate relevant resources across the DNS and Internet.
- It is unclear whether or how needs are already covered by existing entities, how and where any unfulfilled needs should be filled, and what ICANN's role should be.

We suggest that additional efforts to identify those business requirements need to take place via additional ICANN community processes. The workshop may be one input, but its weight should be explained clearly, and we assume the workshop is not meant to be a substitute for wider engagement and more traditional ICANN consultations to come.

The workshop attempted to identify operational requirements via scenario analysis. However, the workshop participants were asked not to raise the wider scope and policy issues that are so closely intertwined with and implicit in the scenarios. This meant the participants examined issues that might not all be relevant, and that the resulting needs analyses may sometimes be flawed.

And while the workshop paper calls the scenarios "issues affecting global DNS stability and security scenarios that would affect DNS stability and security," some of the scenarios definitely did not qualify as such – illustrating confusion about scoping and mission.

For example:

- Scenarios 1.1, 2.1, 3.1, 3.2, 4.0, and 5.1 posit that various parties with delegated authority or point responsibility – such a ccTLD operators, software vendors, registrars, and DNS providers – do not have adequate resources or competence to perform their security responsibilities. This may be true in some cases, but the workshop skipped over the relevant larger issues, and the paper states that a DNS-CERT should help compensate for shortcomings across a wide variety of organizations. The community will need to examine questions such as whether it is possible or desirable for a DNS-CERT to participate in a TLD's operations, or whether a DNS-CERT could be trusted by software vendors of various types across the globe.
- Scenario 2.2 presented the issue of a potentially abusive use of a domain name. It is unclear why a DNS-CERT should be involved in such everyday events, which happen thousands of times a day across the Internet and are often responded to successfully by a variety of good actors. Public comment has questioned why an ICANN-involved CERT should become involved in domain content and legal issues of this nature.
- Scenario 4 deals with a Conficker-like incident. An issue in the Conficker response was that some ccTLDs decided not to participate. The involvement of the DNS-CERT would not have changed those ccTLDs' decisions. Without examination of the policy and social issues, it is difficult to conclude whether a DNS-CERT would have made the Internet any safer than the Conficker Working Group effort did. The further issue was raised whether such infrequent and unique events justify the creation of a new 24x7 response organization.

Attribution: The paper said that "Invitations were sent to the DNS, security policy, and the security operational and vendor community that have participated in recent, global DNS security efforts. These participants are uniquely positioned to both review DNS-specific security responses as well as general Internet security response capabilities," and "Participants represented a wide variety of groups, including ICANN, major ISPs, registrars and registries, vendors, DNS security groups, and the security community."

Attendance was chosen by the ICANN staff, and the number of participants was small in order to facilitate discussion, so it cannot be deemed representative. In the draft we received the nature of the participation and its significance was not identified or disclaimed. The participation of the attendees does not signify that their companies or organizations endorsed the conclusions in the report, or that all attendees agreed with all points. Indeed, some of the participants were there more in individual capacities and were not empowered to make pronouncements on behalf of their organizations. We note that in the paper, "participants" does not always mean "all participants."

We feel that such qualifications are important to state explicitly, so that the nature and significance of the participation is clear and can be weighed by readers. Expert opinion shared in an intimate and focused environment can be conducive and illuminating, but is not comprehensive or decisive.

As a correction: no ISPs were present, and only one registrar was in attendance.

Omissions: A number of salient points raised during the workshop are not reflected in the paper. While limited time prevents us from identifying all of them, we will note a representative example. Scenario 5.1 presents a DNSSEC key compromise at a fictional TLD. We recall how a number of participants discussed how once a ccTLD loses its key, its government and many other parties will be calling the TLD operator and holding it accountable. Participants questioned what role a DNS-CERT would have in this scenario, because a DNS-CERT cannot fix the problem, cannot intervene at the ccTLD or IANA, cannot address the loss of trust resulting from the operator's laxness, and cannot force any parties to participate in after-action studies. The requirements that the participants identified via this scenario might be irrelevant, because a DNS-CERT cannot satisfy them.

Problems with Conclusions: The "response Gaps" section of the paper contains some conclusions and statements that we do not recall being definitively developed or agreed to in the workshop. These include but are not limited to:

- "In short, DNS security requires a reliable, well known and trusted body for all parties to utilize to address DNS security incidents, something which is not met at present. " In contrast, participants noted that response is usually situational, has rarely if ever required a central body in the past, and that relevant trusted parties often do exist. For example, ISC was discussed as a trusted authority in the Kaminsky bug case.
- The paper says that "Another large requirement that is very poorly met in the DNS security community presently is a trusted intermediary or introduction service, which itself has the requirements of an extensive DNS, security, threat researcher, operations and vendor contact list, and also requires trusted communications channels usable by these parties." During the workshop, participants noted how industry bodies and security communities and lists fill some needs adequately, that some parties do have trusted communication channels, and how trust is earned over time and cannot always be brokered. The DNS and security communities cannot have both trust and complete inclusiveness simultaneously.
- The paper says that "Workshop participants generally concluded that dedicated, full time staff whose primary focus was on DNS security could provide those services to the DNS community, meeting those needs, and do so for a larger portion of the DNS world." This statement is too broad, and is unknown if such a thing is possible, especially given that the difference between the DNS community and the Internet community have been poorly delineated.

Again, thank you for the opportunity to comment. We look forward to additional engagement on these important security efforts over time.

With our best wishes,

Greg Aaron
Director, Key Account Management and Domain Security
Afilias

Kathy Kleiman
Director of Policy
.ORG The Public Interest Registry