Top Level Domain Incident Response "Recovery" Checklist

This thought paper offers checklists of actions that a registry operator should perform if the operator's authoritative name server for a country's delegation may have been compromised.

These lists focus on three time horizons: immediate, interim, and long-term actions.

An attempt was made to sequence the activities in a logical order one might expect once an incident has been confirmed, the compromised host and services have been identified, and harmful activities have been contained or have concluded.

While the lists identify resources or specific implementation considerations for Linux running BIND environments, one of the most popular operating system/application combinations for TLD operators, the checklist items are relevant and appropriate for other environments, too.

We do not claim that these checklists are exhaustive. They are offered for reference purposes only, by individuals who have been asked to lend assistance in prior incidents involving attacks against TLD registry operations, without obligation or policy implication.

The compromise of an authoritative name server can create serious technical problems and legal problems, affecting both the server operator and third parties. Nothing in this document constitutes legal advice. Please consult an appropriate professional to obtain advice tailored to your particular situation and circumstances.

We welcome comments and additions. Please send these to dave.piscitello [at] icann.org.

Investigations Basics

If you do not have forensic expertise among your operations staff, we strongly encourage you to seek assistance from professional forensic investigators. Seek parties who have considerable experience who are able to evaluate a potentially compromised system in a forensically sound way, who can identify and preserve critical clues in manners that leave you with evidence that is admissible in a court.

When evaluating a potentially compromised system, forensics efforts will attempt to answer the following questions:

- Was the system *really* compromised?
- What was the path of entry?
- What did the attackers do while they had unauthorized access? Specifically, what has been altered? Deleted? Disclosed?
- What traces did the attackers leave that I can use to identify the (criminal) actor?
- How should I recover from the compromise?
- What are my reporting (disclosure) obligations?

Follow an Incident Response Plan

If you have an Incident Response plan, follow the procedures described therein. If you do not have a plan, notify your own executive team, your legal counsel and your communications or public relations immediately if you believe that you've been compromised. Determine what you intend to report, when, and to whom. (In certain regulated environments or jurisdictions, you may have disclosure obligations.) Designate a spokesperson and make certain that all individuals who are aware of the incident defer to the spokesperson for all reporting.

Reporting Criminal Activity

A compromised system is a crime scene in many jurisdictions. To the extent possible, your goal at all times should be to preserve that crime scene, while ensuring the integrity and availability of that critical server and minimizing collateral damage from remedial operations to domain registrants, their users or customers.

Consult with your legal counsel, but consider cooperating with law enforcement to pursue and prosecute the attackers. Follow lawful instructions you receive from these authorities. Request that all instructions you receive be put in writing to serve as part of your incident dossier: your record of what you did, why, and when.

Preserve the Scene

Follow accepted common practices when you suspect a system compromise:

1. Do *not* turn your system off until you have preserved copies of the system's current state, including RAM[1]. Ensure chain of custody is maintained around the image and copies.

2. Disconnect the compromised system from the network. If you have hot spare servers, ensure that they are online, operational and not vulnerable to the same attack that compromised your primary systems. Place them into production.

3. Immediately make at least two image copies of the system's disks. Once copies have been made, preserved at least one copy in a dated, sealed and signed container. Keep this container under lock and key to ensure that proper chain of custody is maintained and that potential evidence isn't accidentally or intentionally modified or destroyed.

4. Prepare to build a new system(s) dedicated to hosting the authoritative name service. It is not possible to fully remediate a compromised server and achieve the level of full confidence in the integrity of the remediated system that a TLD operator needs. A clean reinstallation or replacement of the system and DNS software is the generally accepted practice. Bear in mind that while less common, some malware may infect BIOS. If you question the integrity of BIOS after your incident, you should replace the system.

Attempt to minimize customer impacts. If you have hot spare servers, ensure that they are online and operational. Swing them into production.

Investigating a compromised system (Forensics)

Follow accepted common practices when you begin your investigation:

1) Use a copied image of the suspect system to:

   a) Review configuration files to determine the extent of the attacker’s infiltration, ideally comparing the current state against checksums or offline copies. Tripwire or a similar product may help with this.

[1] Situation aware attackers may have taken steps to minimize the clues they leave behind. For example, they may be running a remote access trojan (RAT) solely in RAM. If you power down your system, critical evidence may vanish from volatile RAM memory immediately, Similarly, some hacker/crackers may probe for network connectivity on an ongoing basis, and wipe their programs if they notice network connectivity has disappeared. At the same time, if you leave a compromised server online, further damage to domain owners or customers may result, and the hacker/cracker may notice that you're investigating, and also try to cover their tracks.

b) Review file system to identify any file system changes or files the attacker may have left (executables, scripts, libraries, user data). Look also for unfamiliar/unauthorized directories or user accounts, for unfamiliar privileges granted to familiar user accounts, and for process accounting or log information that the attacker may have left behind (for example, lastcomm(1), or vim usage (.vminfo). Confirm that there are no unauthorized secure shell (ssh) preshared keys, or unexpected setUID/setGID binaries.

c) Review log files to identify unusual account, processes, services (especially listeners) and communications activities. (Save at least one time-stamped copy of any original logs, whether tampered-with or not).

d) Review zone file data. Compare against the last known-to-be-correct zone data to identify any unauthorized changes to resource records of authorized delegations. Also look for any resource records that may have been added without authorization.

e) If an external party reported the compromise, collect as much information as possible about the way the party determined that the name server was compromised.

Document all your findings. The goal of (a)-(d) is to identify, if possible, the attacker's means of entry and attack methodology. Take notice of and record times of incident-related activities to construct a chronology of the event. Where possible, complement this dossier with information from event logging performed at other infrastructure systems (routers, switches, firewalls, database servers or other services).

Restore Authoritative Name Service (DNS): Configuring the Operating System

Continue forensic investigation on a copied image of the compromised system. In parallel, separate critical DNS-related operations from other services by building an infrastructure where you can operate authoritative name service on a **dedicated host**. Authoritative name service is a critical function and should NOT be run on a shared system.

2) Build a new system dedicated to operating as an authoritative DNS server.

   a) Erase hard drive, install operating system, and bring OS to full patch currency. If you are re-using the compromised hardware, overwrite the BIOS using the latest manufacturer's BIOS image.

   b) Create new root/admin account passwords (apply current recommended practices for password composition complexity rules). Add some form of multi-factor authentication. Limit access to only those accounts that will be used to manage authoritative DNS, including limiting access to the system from a minimum set of allowed IP addresses associated with authorized users.

   c) Enable unattended-upgrades: critical security updates are usually safe to deploy unattended. (Overlooking a critical security update may have more severe consequences than a service disruption from a failed update.) See Debian and Ubuntu (called AutomaticSecurityUpdates) for details or search for your OS of choice.

   d) Setup Secure Shell for encrypted remote access. Ideally, use key-based authentication but if you must allow password logins, then use fail2ban or similar methods to mitigate brute force attacks. Whitelist authorized IPs and users. Use client certificates to strengthen authentication. See SSH/OpenSSH/Configuring for details. Choose server-side and client-side ciphers/keys wisely, since the default ciphers and seeds are thought to be weak.

   e) Reduce the attack service by disabling all non-essential services. You may also want to remove non-critical packages. See ReduceDebian (Skip the removal of IPv6 files).

   f) Set up system monitoring. Consider running logwatch, tripwire, and a system firewall, see IBM's Hardening the Linux Server for details.

   g) Enable process accounting. This is provided by the psacct and lastcomm command, available in the 'acct' package (apt-get install acct), see this process monitoring resource.

h) Enable system auditing. See this Linux server hardening resource.

i) Consider implementing currently available Linux security extensions.

j) If you do not have a dedicated log server, build one. See Creating a Centralized Log Server if you intend to use syslog-ng or this RedHat documentation for rsyslog.

k) Configure remote syslog. See this NSRC log management resource for further guidance.

Set up authoritative DNS for your delegation: Install and Configure BIND

3) Build a new authoritative DNS server.

   a) Install your DNS server software. Bring to full patch currency. Review these guides that describe a BIND9/Ubuntu installation and how to set up DNSSEC. Run BIND9 as a non-root user, chroot BIND, and log BIND audit trail.

   b) Do not copy any files from the compromised system over to a new server that will replace the compromised system. The intruder may have modified these. Create new ones, or, if you can determine the date and time of the compromise, use files from a backup taken before the incident occurred.

   c) Configure DNS server as authoritative. This tutorial describes a representative authoritative server configuration.

   d) Disable recursion to protect your authoritative name server from DNS cache -related issues and attacks against caches

   e) Prepare zone data. Do not edit the zone data on the authoritative DNS server, but instead, set up a process whereby the "last known intended zone data" is maintained externally from the authoritative DNS server and uploaded to a hidden master and then synchronized across primaries and secondaries. See this NSRC resource for a representative implementation.

   f) Enable zone file audit trail. PHIL can you explain your notes on this recommendation?

   g) Enable checks to verify zone integrity. Use "EOZ TXT" or similar marker records in the zone to make sure the zone hasn't been truncated (out of disk space conditions, etc.). Consider using checksums.

   h) Configure DNS server logging (for BIND see NSRC's logging recommendations for some ideas but modify to use remote logging as described earlier.

   i) Run Network Time Protocol (NTP). NTP should be secured. This Team Cymru template shows configuration options and iptables rules. Synchronize time across DNS servers, security systems, and syslog host.

   j) Monitor the authoritative server to detect unauthorized zone changes, see section 7.2 of ICANN SSAC 044.

Document each step of your installation. Save copies of your intended configuration files on a host separate from the authoritative DNS.

Recover and Restore Other Affected Services

[Note: this section may not be relevant if the compromised system only hosted authoritative DNS.]

Compartmentalizing services protects your authoritative DNS from attacks that use a web, mail or other exploit for access. For example, many dynamic web applications may have vulnerabilities that can be exploited to gain administrative privileges on that server, undermining the security of critical authoritative DNS services. If the compromised system hosted other services, move these to a separate server(s) from your authoritative DNS. You should also segregate these other services on their own network (LAN segment), away from the network segment you've reserved for your authoritative DNS server.

To recover and restore other affected services (and in some cases, to identify the attacker's original path of entry), continue forensic investigation on a copied image of the compromised system. As this section describes recovery activities not specific to authoritative name service, it only highlights select recovery activities.

4) Conduct forensics on all services that were hosted on the compromised system.

   a) At a meta level, this iterates 1(a)-1(c) for each service.

   b) If legal authorities insist that you leave the system up to investigate,

      i) Add countermeasures to ensure that the attacker cannot disable remote logging or extend his attack to other systems or networks.
      ii) Add measures to block any malicious traffic that the attacker may attempt to generate from the compromised system.
      iii) Consider putting in place honeypots, canary accounts, or other methods to track future activities of the attacker.

   c) Install services on the new application servers. Take this opportunity to review and prune unneeded services that may be operating on these hosts.

   d) Synchronize time (use NTP).

   e) Enable remote logging.

   f) Generate new digital certificates for secure services such as HTTPS.

   g) Configure user accounts. Enforce a strong password policy by implementing password complexity.

   h) Notify authorized users of the event, provide instructions for remedial actions they should take, or any changes that affect user configuration as a consequence of segregating services to separate systems or LAN segments.

This Is A Living Document

Current, accepted, or recommended practices may change. We welcome your suggestions for improvements or updates.

Contributors

David Piscitello, ICANN
Janelle McAlister, Mark Monitor
Justin Mack, MarkMonitor
Dean Pemberton, NSRC
Phil Regnauld, NSRC
Bill Haigh, .PN Registry
Joe St Sauver, Ph.D., Farsight Security, Inc.