Global Information Assurance Certification Paper

CodeRed II: Incident Handling Process and Procedures.

> CodeRed II was discovered on August 4, 2001. It has been called a variant of the original CodeRed Worm because it uses the same "buffer overflow" exploit to propagate to other Web servers. Symantec AntiVirus Research Center (SARC) received reports of a high number of IIS Web servers that were infected. CodeRed II is considered to be a high threat." (Szor, CodeRed II)
>
> When a host gets infected it starts to scan for other hosts to infect. It probes random IP addresses but the code is designed so that probing of neighbor hosts is more probable. If the infected system has the language set to Chinese the worm starts more aggressive scanning (600 threads instead of 300). The scanning runs for 24 hours after the infection (48 for Chinese machines) and then the system is rebooted. There is a time limit in the code that will stop the worm on the 1st of October. At that time it will reboot the machine and stop spreading. The installed trojan still remains in the system! (Erdelyi, Code Red)

CodeRed II was a wake up call form many corporations. The virus caused internal networks to slow down or stop and deposited a back door onto the system. Clean up and patching of the servers was in theory quite easy but proved difficult and time consuming in reality. Unlike a mail virus there was no central location that you could run a program on (such as the mail server) to clean or contain the virus. CodeRed II was targeted at IIS web servers but a large number of laptops running Win 2000 Professional (which happened to have IIS loaded on them) were also hit.

CodeRed II was a great primer for most corporations on how their incident response processes and procedures worked. Many corporations had hardened their external web servers but left internal servers and workstations vulnerable. The assumption was that corporate firewalls would stop the spread of viruses such as CodeRed. This was a false assumption because a single laptop taken home by an employee and infected outside of the corporate enterprise would circumvent the corporate firewalls. The laptop may have virus protection loaded on it but if the most recent virus definition files loaded on the laptop did not recognize the new virus the laptop would be infected. When it was brought back to work and plugged into the corporate enterprise it would infect machines that resided inside the firewalls.

The 6-step method for incident handling is to prepare, detect, contain, eradicate, recover, and lessons learned. This paper uses the CodeRed II virus as a template to generate questions to help you better prepare for the next virus outbreak. We will use lessons learned in each of the steps to better prepare for future virus infections.

CodeRed II could have been much more destructive than it was. The nature of the virus allowed enterprises to clean up and patch systems without an immediate time constraint. The virus was not destroying data and as it spread but the next one might. I will go through the detection, containment, eradication, and recovery steps that were involved in the systems and raise questions that you need to think about. I will suggest some answers but at this point the questions are more important. The correct answers will be different for each company based on the corporate structure, culture, and tolerance to risk. The questions brought up will focus on processes and procedures.

Technical solutions are easy compared to the actual processes and procedures that are employed. In most companies this aspect is given the least amount of time. Everyone loves the technical solutions and will minimize how the technical solution will be implemented. This is understandable since major outbreaks do not occur frequently so most companies do not have a live test in production and do not understand the problems that they will run into. Testing in a lab is always different from production. For this reason we should capitalize on the CodeRed II outbreak experience and treat it as a production test case.

The first order of business once the enterprise has been breached is to identify infected machines. How do you identify infected machines if you have been infected before existence of the virus becomes general knowledge? With CodeRed II this could have been done by the increase in network traffic. If your network starts behaving differently than expected it is safer to assume that you may have some kind of virus propagating. What does your network staff do at this point? They may very well follow their standard procedures and reboot routers causing logs to be wiped which could have been used to identify machines that have been infected. Do you have any network engineers that are trained to handle virus issues? If they suspect a virus do they have any procedures for reporting or testing to confirm? The earlier suspected activity is detected the better. You may have intrusion detection software but is any effort put into training the network administrator on what to do if they notice something funny? If a virus has been written to evade intrusion detection software then having a person noticing something odd may be your only chance to catch it early. The CodeRed II virus caused the network to be flooded by the infected machines scanning for new machines but what would have happened if it had been subtler? The opposite also applies, if the network was flooded did everyone assume that it was a router issue causing the problems wasting hours or days before checking for viruses? Have *easily* followed procedures for administrators ready to follow if any suspicious or strange activity is noticed.

On CodeRed II some companies used eEye Digital Security's CodeRed Scanner. This would mark machines running IIS as infected or vulnerable. It would report the status on machines by IP address. This leads us to the question that if you are going to use a scanner such as this can you reach all of the subnets in your enterprise? How do you scan machines behind firewalls? Do you have a procedure to do this or some policy that allows access to all subnets under certain conditions? If you miss one subnet you might have hosts re-infected that you thought were clean.

Once the IP addresses of infected or vulnerable hosts have been identified the host names must be resolved to the IP address as well as the ports and physical locations of the hosts must be identified. If the infected machine is a production machine with a static IP address chances are that you know where to find it. If it is a laptop and gets its IP address dynamically it can be considerably more difficult to find it or the owner. Do you have any documentation on what subnets exist where? If you have Vlans do you have the locations documented? At some point you may need to actually do a physical walk or trace the wires to find the machines. You want to have this information on hand before an outbreak, trying to gather it during an outbreak can slow down your progress. It is worth the effort to keep this information updated and easy to access.

Once you have IP addresses can you attach names or ownership to the box? If it is not a production machine you may not have rights to the machine. NBTSTAT can find the machine name given an IP address. DNS lookups can gather machine names for you as well as the wins database and the DHCP database. Doing name lookups manually is effective only in small outbreaks. If you have hundreds of machines involved this task becomes time consuming and error prone if done manually. Maybe you can have a programmer code up a tool or buy one off the shelf that will do the name resolution for you quickly and gather basic information on the system. Trying to identify machines is not a trivial task. You can use tools such as Hyena (for NT servers) to pull accounts with admin rights on the machine (if null enumeration is not turned off) to get people to contact. Better yet is to have policies in place with naming standards and a policy regarding domain memberships and who has rights to the box. This is when system management tools really shine if deployed enterprise wide. Remember, you have to also think about your worldwide WAN links. If you have any asset management systems in place this would help in tracking owners of machines.

Do your network personnel know how to disable ports on routers, switches, or hubs? Do they know how to do it across the corporate global WAN? Do they have the rights and authorities to disable ports at other corporate locations? These are some of the questions that must be asked and procedures and processes put in place for disabling ports, subnets or networks. Knowing how to disable the ports is not enough; your network personnel must be able to disable them quickly. If it takes 45 minutes to disable a port and you have a virus quickly propagating throughout the enterprise network you may not be able to contain the virus on a port-by-port basis. You might be forced to shut down entire subnets or networks. This is critical on a virus like CodeRed II that has the ability to quickly spread to other servers. The quicker you can get infected boxes off of the wire the easier it will be to contain. Disabling a port is generally quicker than trying to physically find a box and shut it down. If machines get their IP address dynamically, can you keep users from switching the box to a different network jack and getting back on the wire? This highlights the need to find names to associate with the IP addresses. If the IP changes you can still track the machine. You must have procedures in place to deal with this situation.

If you cannot contain the virus through disabling individual ports do you have any general contingency plans in place to stop widespread infection? If you have a typical large corporate network it could take you days to weeks to get agreements from various groups or divisions about shutting down sections of the networks. If a potentially destructive virus is introduced it is critical that you be able to act quickly to contain it. If you do not have contingency plans in place that have been approved by upper management a manageable infection (if reacted to quickly) could quickly evolve into a nearly unmanageable one in a matter of days or hours. Know what you can and cannot turn off before a crisis occurs. Having the CEO sign off on the policy helps to quickly settle disputes during the crisis situation.

Once you have determined that you have a problem someone must be tasked with doing research to discover if this is a new virus or an existing one. Ideally relationships or agreements with Security companies should already be in place so that you can quickly determine what you are dealing with. In today's world you cannot rely completely on in-house staff to be able to identify new viruses. You must set up

relationships with commercial vendors or agencies early to help when the eventual infection occurs. If you are having a problem chances are others are also having it. It is vital that you be able to identify the signature of the virus infecting your enterprise. It may be as easy as searching the web or as difficult as getting experts in to review an infected machine. Getting a signature of the virus is important because if you have been treating it at the network level your are only seeing machines that are showing symptoms of the infection not machines that are truly infected.

If a signature can be identified you must have some way of checking all systems that could be infected. You must be able to identify if the machines are infected and if they are vulnerable to infection. You may need to have a programming resource available to code detection tools if none are available yet. In the CodeRed II infection the signatures were known and tools were available that could be run to determine if a system was infected and vulnerable. These tools were not perfect and would report unknowns as not tested in which case a further determination would have to be done. Without some way of automatically checking you will never have any confidence in the level of infection or cleanup. Employing manual procedures for checking for file infections are to slow and error prone to be useful in a large corporation. You may have to verify 10's of thousands of systems.

Having a tool is the first part to detecting the systems. Being able to run the tool on all of the systems is the second step. Many corporate LANS have firewalls placed throughout the enterprise. These may block your detection tools. Team members running the tools may not even have rights into certain network segments. Processes must be present to either open up the firewalls or to physically attach to the protected zones for detection. Do you have your protected areas documented? If you do not know where the protected zones are you may not know if you have missed whole subnets in your detection scans. Labs that may not be physically attached to your enterprise network are another area that must be dealt with.

When a crisis situation arises it is helpful to have a team already formed and on standby. This crisis team should meet occasionally to do some mock drills throughout the year. Backups for the team members need to be identified in case one or more primary members are not available. It is vital that all members of the team be completely dedicated to the containment and clean up of the outbreak during a crisis situation. Having a team member pulled out to finish work on some other vital project can slow down the containment and clean up by days if he/she is a critical team member. You need to have policies in place for dedicated team members.

The mix of skills in the team needs to be varied and come from all possible groups involved. You need more than just your administrators. You will need technical people and non-technical people. Some of the skills you might need are Project Manager, security specialist, Network engineer/administrator, server engineer/administrator, programmer, executive management representative, business specialist, legal representative, corporate communication representative, help desk representative, database administrator, and extra bodies for any work that requires mobile people out on the campus. You have to plan and scale for the worst-case scenario. It is easier to scale down a response then it is to scale up to it.

A project manager is needed to manage the situation as a whole. If you let your technical people try to manage a breakout then you are taking them away from their

core competency and chances are that things will fall through the cracks. The project manager is vital for being the center for all information and setting deliverables and time frames for team members. The project manager will report regular status to management and allow the technical people to keep working. It is extremely easy to have multiple people doing redundant work without realizing it. A project manager will coordinate all members and allow them to work efficiently together. If a project manager is not available a team member will need to be assigned this task. This is a full time job so it is important to make sure that the person is dedicated to managing the outbreak. If they start getting heavily involved in the technical work there will be no one who is able to step back and keep from getting tunnel vision.

A Security specialist is needed to understand the outbreak and to make recommendations on containment, signatures, detection, etc. Server engineers/administrators are needed to gather information and do anything that requires rights on the servers. Depending on how your support is set up this could include web administrators, database administrators, etc. The same holds for the Network Engineer/Administrator. You need a person with the skills and rights to take action on the networks. These network engineers are critical in an outbreak such as CodeRed II. Subnets become flooded and the network can come to a standstill. Users will be screaming and you will need to take actions quickly. This can include running network traces, disabling ports, reconfiguring firewalls or routers. This is the person/people that can make or break the day. Make sure that the team member is a high level technical person with all the appropriate rights who understands the enterprise network completely. If you have procedures in place in case of an outbreak you do not waste time discussing what should be done. You will know what to or at least have a general game plan.

It is very helpful to have an experienced programmer on the team. As the outbreak first occurs you will need to gather information about systems, files, and look for virus signatures. If a tool has not been developed to locate infected machines by the time of the outbreak the programmer can code something up or script it out. This can save massive amounts of time. The same applies for patching, changing system configurations, and verifying cleanliness of systems. The less manual work that you have to do the quicker you can get everything under control. The programmer should be skilled in several coding and scripting languages. You do not need a coding genius for this slot but he/she must be able to think quickly on their feet and code up short programs or scripts on demand quickly.

As the team works to contain the outbreak an executive management representative needs to be involved to approve of decisions made by the team. If routers or networks need to be turned off it would be the executive manager representative that would give the approval. You do not want to bog the team down with eliciting different managers for approval. The executive management representative has to have the authority to make decisions quickly for the company as a whole. Ideally this person should be on the board of directors.

If the team is going to make any changes you need a representative that understands your core business and what the business fallout will be for incorporating any suggested changes. If you turn off or drop off of the wire systems will there be financial impacts. There may be an obvious solution from an engineering point of view

that may be completely unacceptable from a business point of view. If the solutions bankrupts the company or harms the company name you might be better off living with the risk of not shutting down or cleaning a system. In the same vein you will need a legal representative to handle the consequences for missed service levels, possible breaches of contract, what actions that can be taken, and how to phrase any communications. One team member needs to be able to send out communications on a corporate level to control rumor and manage the information that is supplied to the employee population.

The last thing that you may need is a pool of workers who can roam the campus and clean machines, find machines, or help users as needed. These individuals can do any of the general work that is required so your specialist can concentrate on what they do best.

Now that the virus has been contained and you have started cleaning up systems you will need to decide with what level of risk you can live with. In the September issue of Microsoft Certified Professional Magazine there is an article that will let you quantify risk. In the case of CodeRed II the payload allowed remote access to the system. The recommendations of security experts was that the only way to be absolutely sure that your systems integrity had not been breached would be to format the drive and start all over. At this point it is important to think things through. If you format and re-install the operating system you will have a clean system but how long will it take to restore the mission critical applications on it? If you restore necessary data back to the system you cannot guarantee the system integrity unless you can absolutely identify the date the system was infected. The payload may have been sitting on the system for months. What is your policy for infected machines and is it realistic? CodeRed II was fairly benign and if you had a strong confidence level that no other Trojans were deposited besides the ones reported you might feel comfortable enough to just clean and patch the infected systems. The more systems that are involved the more likely that the drastic measure of re-install will not be realistic. Your security team may want to keep the disks that were infected for forensics or prosecution but if the system is vital then it may be better to just get the system back up as quickly as possible. Here is a situation where there is a good chance of conflict between 2 groups. What is the policy in a situation such as this?

Your response team has contained and cleaned up all infected systems. It was a success and everyone including management is happy. Are you through now? No, CodeRed II has been stopped but new machines will come onto the network as the months go by that are vulnerable. An employee on vacation will come back to work with his/her laptop. Old machines will be rebuilt and someone will forget to install the patch. The fight never really stops. The response team must put procedures or tools in place that will periodically scan or verify the integrity of all of the systems. As other viruses come into play this will get more complicated. You cannot depend on virus protection alone because things can slip by. Once the initial infection has been put down it is normal for vigilance to go down after time. Now is the time to think about the future. Do not wait for another outbreak. If you put manual processes in place can you really expect them to be followed in 6 months or later? Any process or procedure that you put into place has to be realistic. You can state that someone will check for additions of files on the c drive but unless you have it automated it will not get done

after a couple of weeks. It looks good on paper but will be a failure point later on.

All of the above questions need to be thought of when you develop your policies and procedures. A very useful tool to have or create is a “rules of engagement” document. This needs to be short and concise. Keep it to a few pages at the most. If your document is a book then no one will ever read or use it. This document needs to spell out what you can and cannot do when an outbreak occurs. It should answer such questions as: “Can you commandeer staff to fight the outbreak?”, “who gets communicated too and when during an outbreak?”, “which systems are vital and need special considerations?”, etc. It will state which systems you can take off of the wire and which ones you absolutely cannot. When you are in the middle of an outbreak and speed is of the essence it is to late to start debating what you can do. The more questions that you can answer in the document (based on your experience) the easier it will be able contain future outbreaks. This document needs to be a living document. You need to have as much information as possible without writing a book. The longer the document the less likely it will be updated. Try to make it useful and concise. This is not the place for extraneous words or sections. If detailed information is required add a link to it in the document. The purpose is to make it useful and used.

The more things that you can prepare for ahead of time the better off you will be during a crisis. You do not want to be handling a critical situation by the seat of your pants. Once you define the core policies and procedures it should apply to a wide range of different types of attacks. The CodeRed II virus is a great tool if we take a look at what happened and use it as a template to change what needs improvement.

Bragg, Roberta. “Risky Business.” Microsoft Certified Professional Magazine September 2001 (2001): 28-40.

“CODERED.B.” Virus Encyclopedia. 31 July 2001. URL: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=CODERED.B (5 September 2001).

“CodeRed Scanner from eEye Digital Security.” 5 September 2001. URL: http://www.eeye.com/html/Research/Tools/codered.html (5 September 2001).

Erdelyi, Gergely; Rautiainen, Sami; Hypponen, Mikko. “Code Red.” F-Secure Virus Descriptions. August 2001. URL: http://www.datafellows.com/v-descs/bady.shtml (5 September 2001).

“Microsoft Security Bulletin MS01-033.” 20 August 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp (5 September 2001).

Northcutt, Stephan. “Core Issues and Challenges.” Information Assurance Foundations – SANS GIAC LevelOne. 13 January 2001. URL: http://giactc.giac.org/cgi-bin/momaudio/s=1.1.1/a=r4ogh7IuZcz/iafoundations (5 September 2001)

Szor, Peter. ”CodeRed II.” 4 September 2001. URL: http://www.sans.org/giactc/GIACTC_citations.htm (5 September 2001).

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event