OARtech 4/13/2005

Introductions

Oarnet Update
Linda Roos

Linda introduced Pankaj Shah as new Oarnet director. He was with Oarnet before as the ITEC director. He has been back with Oarnet about a month.

Pankaj Shah, Director
Glad to be back. Ohio is at the leading if not close to the bleeding edge in networking. Feels this is a great opportunity for us. We need to look for collaborations and ways to work together. If you have projects you have "shelved", now is the time to bring them out work on them. This is OUR network and that's the challenge. There is a vast different between renting/leasing and owning.

Paul Schopis, TFN/Oarnet Update
(Slides available at: http://www.osc.edu/oarnet/oartech/presentations.shtml)

Pending Fiber Builds
The following schools are building connections Kent State University, NEOUCOM, Springfield, BGSU, and Youngstown State. Kenyon has come in to Nielston pop via Time Warner. Remember that all schools are now sending traffic over the TFN. OIT is looking to use the old POPs so Oarnet may not retire the older POPs.

Retiring of the old backbone lines is near completion.

They are working toward having a menu that is selectable for research resources.

Partners - Schoolnet parts are in the warehouse and the deployment schedule is being developed. OIT has a new interim director, but the signing of the contract is delayed some.

Current Projects - Netflow results are due 4/15/2005 and they feel they are on schedule and are looking at options for traffic classification. The worst circuit has been resolved - they had a DS3 that was working improperly. They finally got it to work after about 2 months. They will continue refining the BGP prefix listing.

Security
Patti Vendt

EDUCAUSE security conference overview: Cal Frye and Brian Moller attended.
There was more of a holistic approach to security. They looked at layering security and taking it deeper into the organizations. There was interest the amount of funds that were being spent on security. Risk assessment tools: Octave, CIS. It was a good conference

and recommend people look to attend next year. There was session on how cracking works, legal issues, risk assessments, and the need of a whole look at security. State of Ohio has created a special counsel to help education with Graham Leach Blyly.

Security Presentation
College of William and Mary
Norman Elton, Matt Keel
Slides available at: http://www.osc.edu/oarnet/oartech/presentations.shtml

A BOT is a piece of software that connects back to a centralized control channel and allows unauthorized control of many machines from a single point.

BOT Lifecycle:
Starts with the initial infection and payload, then talks to command and control server, then they get an additional payload, and start scanning your local network. Then all the infected machines start the lifecycle again.

Initial infection
BOTs are seen the most on unpatched operating systems with remotely exploitable vulnerabilities. Initial infections are reduced if the machines are kept up-to-date. The biggest problem is the social engineering used to trick a user into downloading a payload. The payload doesn't exploit vulnerabilities on the system, but vulnerabilities in the user. Methods are embedded payloads in popular downloads, sending email from an infected PC, sending IM to all friends on a buddy list, and changing a user's IM profile or away message. This last method is particularly prevalent on campus networks. It fools the user into thinking that someone is offering pictures, or other information from a friend's away screen (pictures, etc), the user clicks on the link to see the pictures and the executable is installed. Types of payload include EXE, SCR, PIF, GIF/JPEG when the display engines are found vulnerable. The payload is delivered via HTTP requests to a compromised web host, occasionally FTP, TFTP, EDCC, CSend, and perhaps P2P. They haven't seen it a lot in P2P, but have seen some and it is hard to find.

Command and Control
The BOT allows control of many hosts from one system and is typically done with IRC. They have some reports of Yahoo Messenger being used. It is usually a hard coded channel and IP for the server in the payload. When a server is removed, they just remove the IP from the list and the traffic is failed over to, other IPs. Once online, the BOTs wait for commands from the botmaster. It does nothing without the botmaster giving the commands.

Typical Abilities
BOTs can download additional payload to exploit new vulnerabilities. They transfer files to/from the infected host and spread the infection to the local network often bypassing firewalls and IDS. They have seen massively coordinated port scans often for reconnaissance for future attacks. Lots of BOTs open spam relays, SOCKS proxies, log

keystrokes to harvest bank info (especially for PayPal). They are seeing more spy ware being installed.

Motivations - Entertainment, pride (I can infect more systems than you), revenge against another BOTnets (BOTnet theft is not uncommon), using the BOTnet to jumpstart a worm outbreak and money. Money has become big in the last year. They earn money by relaying spam, corporate extortion, PayPal account to drain accounts, or exchange money with others, stolen ATM card use, and rent-a-network (rent a BOT network). Spy ware installation is often paid on per installation basis and they are paid more as users view/click on advertisements. There is a tracking mechanism in the spy ware (usually a string of numbers) that can track it to the BOTnet.

Detecting infected machines
NIDS Signatures - IRC Joins (commands going from one resnet to another resnet), PIF/SCR downloads they found raises a red flag, looking for common BOT commands (e.g. aim.goaway, .advscan) and backdoor or shell commands. Make sure the signatures are not restricted to common ports. Check DNS logs for queries for known bad host named or domains. You can also look at flow logging for port scanning and inbound IRC as well as connections to known command and control IP addresses.

Researching an infection
First goal - find the command and control DNS name (use Linux or macs, they do not use windows boxes for this).

VirusTotal site is a good site for find the virus variant. Norman AntiVirus Sandbox can take the virus and tell you about what that virus is doing to the infected machines. Strings pulls out the ASCII text from the virus so you can find references to the source and person name to a variant.

Sometimes they run the payload in a monitored lab, but often the payload will not functions inside VMware/Virtual PC.

Quarantine the infected hosts to VLAN, disable the network jack, or use Netreg. Block access to the payload using acls or Packeteer to redirect the web requests for a particular payload filename. You can also poison the DNS resolution of the payload server. He showed a sample Packeteer configuration and showed an example of DNS Poisoning. You could poison the address to point to themselves, or to a sniffer.

There is no complete cleaning of the infected machines. Best practice is to format and reinstall the operating system. Users must change all passwords as they are suspect as having stolen by the BOT. Antivirus software can't be trusted to clean a BOT.

If you must clean a machine, then use the results from Norman AntiVirus Sandbox, use regmon, filemon, rootkitrevealer and others from sysinternals. Remember that the BOT may have downloaded additional payload beyond the original BOT. When the PC is

reconnected, monitor it and look for suspicious traffic. Note this takes a lot of time. There is a tool called DNSwatch that will watch for known command control IPs: aharp.ittns.northwestern.edu/software. Use this to watch flows logs. Away hunter, www.awayhunter.com, shows the sites that have the away message payloads. Sometimes you can do a zone transfer from the domain and you can get additional names in the domain to allow you to block the traffic (showed an example): dig @SOA -t AXFR domain.name.

To remove the payload use whois to get contact information for the site hosting the payload, check the website for contact info. Be polite and include log files in email. Be ready to explain why the file being hosted is bad. You may have to remind them that antivirus software doesn't always get the BOTs. You may have to check to see if the file returns indicating the entire server has been compromised. To shutdown the command and control use whois to get contact information for the site and explain they are running an irc server that is coordinating a BOT network.

Ultimate technique is to remove the DNS record. It takes time, but a can disable the entire BOTnet. You have to contact the company that are hosting the DNS records and can be found using dig and whois. Coordinate with others to help in convincing the DNS provider to shutdown the domain. You want the domain name flagged so it cannot be used again for at least a year.

Coordinating with others:
University Security Operations Group: www.dshield.org/mailman/listinfo/unisog
Internet Storm Center: isc.sans.org
Research and Education Network ISAC: www.ren-isac.net
Incidents Mailing list: www.securityfocus.com/archives
Windows-HiEd: www.windows-hied.org

Working with Law Enforcement - They worked through their campus security and then with FBI. Ultimately you would work with FBI as they have the jurisdiction. Save All log files, document your investigation and be ready to estimate the damages (bandwidth lost, cleaning hours, productivity loss).

They see problems in the future coming from encrypted command and control communications and payload deployment via P2P. These will be hard to find and block.

Caveats: Get permission before logging of DNS queries, IRC traffic, and flow records. Connecting to a command and control by impersonating a BOT is a sure way to get DDoSed. Trying to hijack a BOT network and issue an uninstall could cause damage and is likely illegal.

References:
www.nanog.org/mtg-0410/kristoff.html
www.honeynet.org/papers/bots
asia.cnet.com/enterprise/infrastructure

The presentation is also available on www.educause.edu.

Email addresses:
Norman Elton norm@wm.edu
Matt Keel matt@wm.edu

One school has blocked IRC unless the user has actually requested to be allowed through. Thus anyone using IRC that is not one the list could be doing bad things. This approach is rough, but it has worked for them.

The Security forum is available. Patty has sent some security survey information to put on the forum. If people want an account you should contact Patti. They have found that they had to update some of the university contact information as the request must come from the official OARtech contact for the university. They will have more to say after the lunch.

Next security presentation will be Doug Pearson from Ren-Isac (Research and Education networks for home security)

PGP signing party
Several OARtech members participated in a PGP signing party. Each member confirmed his pgp fingerprint to the other members. Ransel then signed each member's public pgp key, and sent them all the exported public keys. What Ransel really likes about pgp is that it can be utilized to securely store account information, even via email. PGP is becoming more common and they use it to control root access to administrative machines. If you wish to get the keys, you should get Ransel's key at least so that you can verify information coming from him: http://net.kent.edu/~ransel/Ransel-Yoho.asc

OhioLink Shibboleth Authentication: They are currently cleaning up the scripts and are hoping to have server available for testing in the next month or so.

Lunch

Packeteer update
Sean Applegate
Slides are available: http://www.osc.edu/oarnet/oartech/presentations.shtml

Contact info:
Sean Applegate
Mid-Atlantic Territory Engineer
703-801-0413
Sapplegate@packeteer.com

What's new in 7.X

Several minor user interface improvements that allow for page sensitive help with unit information and a change to a horizontal layout on the menus. It also has tree depth control to help getting through the filters. Quick commands page help you by allowing you to select, move and edit commands with selection of classes from a list of defined classes.

IP Filters can allow telling the unit to ignore specific IPs or only accept specific commands. Command would look something like:

ip passthrough main outside src 192.168.32.1

The "ip show" command shows the filters. This command is not documented. There is a bug that if it deals with too many subnets, it can cause the box to reboot.

Flow Detail Records allows you to see the flow detail records. It typically increases cpu usage by 5-10%. Collectors can use a V5 flow collector. The flows come in v5 format with class information. Packeteer 2 gives you much more information about the packets. This will allow you to actually see application names instead of just port numbers. To turn it on go to the setup page and enter the collector IP information. It can also be turned on in command mode.

Adaptive Response allows you to setup SLAs that gives you a notification when something has happened. It uses templates, agents, action files, and incident reports. The goal is to make it smarter. The templates identify the metrics that can be monitored for a specific variable. The agents are the glue to connect the actions files with the template to the action files and incident reports. An example use would be if a site uses a large amount of bandwidth for a long period of time it acts to limit the bandwidth and can notifies another party.

Default templates are available to help you act on specific issues such as default traffic limits, new applications, and high bandwidth hogs.The general variables allow the unit to act on any variable that is measured. The health templates will notify you when it detects that it is not functioning at a healthy rate. To implement these templates you would go to the AR Dashboard. There are agents that are setup by default that measure the alerts, but have no action on them. You may need to adjust the thresholds. He showed an example of setting up an adaptive response for a bandwidth hog rule.

DoS Tuning
What to look for on the packetshaper include host flow failures (Hostdb info –sp -n 10), Tcp-inits, Tcp-server-ignores, client-floodblocks, Server-floodblocks, tcpallocfailures, and hostdballocfailures. If you see floodblocks or allocfailures your box is having problems keeping up. The report portal allows you to setup a page for quick lookup of these variables.

Load shedding allows you to drop new and/or existing connections on a per host basis that exceed certain parameters. He showed a sample for implementing load

shedding. You would first setup the exceptions and then setup the thresholds and turn it on. Very similar to policy flowlimit, but flowlimit is not as efficient. Flowlimit is setup by default but the thresholds are fairly high so you don't notice them.

You can't do adaptive response on the 4500 due to memory limitations.

Performance tuning basics:
Hard code interfaces; prune your traffic tree; increase discovery thresholds; turn discovery on sparingly (schedule it); classify/shape resnet, admin, library, labs separately; use partitions and policies together; use rate policies on medium to long lived flows: don't use rate policy on/_bound/default classes; protect and limit traffic; use scheduling as appropriate and backup configurations or do time of day shaping; and don't run your device at 'Red Line' thresholds. There are some companies that can do tuning for you. Advanced configuration includes configuring adaptive response for system health and setup the report portal for customer performance variables. Using this you can look at the parts per thousand that the machine is working with and then identify possible issues in your traffic. Undocumented command for memory allocation issues: "sys kmem types" or "sys kmem pkt buffer". Watch the failures on this page.

One site has had problems with the 4500s during an attack.

How to get P2P that is falling in the default bucket? Check for memory failures to see if magic is getting any failing. Often this happens if the box can't keep up. Every 15 minutes the packet shaper runs a diagnostic file. Sometimes this can cause a noticeable hit on performance on a box that is running near the limits.

They now have 10K box and 9500 box. Normally it is DDoS attacks that push the box over the edge.

Suggestions from the group include someway of classifying games and allowing them to run. It would be good if you can find a list of valid ports used by games so you can setup a rule for them.

Is 7.0 BGP aware? No.

Next generation is being developed right now with a Linux like operating system with blades to allow you to add/upgrade modules without modifying other modules.

There was some sense that the support center performance has declined some this year. Don't be afraid to ask that a call to be escalated to a more senior engineer if necessary.

Are you interested in CBT? No response from the group. There is an active response training video available from Packeteer, also a certification program. If you purchase services from third party be sure they are certified. He talked about some of the new boxes that will be coming out. Eventually these will phase out the 2500 and 6500 boxes

though these boxes will be around for a while yet. First next generation box should be available in about a year. They are moving away from a feature oriented screens to work flow oriented screens. 7500 will be comparable to 9500. CPU and memory will be higher in the new systems. If you are looking to upgrade it might be best to wait 6 months or so and buy the new boxes. The next generation boxes will be able to pick shaping policies based on class of service and are able to rate limit as well and can also use MPLS labeling. There may be some trade-in policies developed for the new boxes.

OARtech portal
You will have to log into the security portal. Patti will be sending the information to each person that requested an account. There will be a survey on the portal for each site so we can discuss security issues in various subject based forums.

Barbwire is a spam/virus product that a couple of sites have had problems with, in fact one has removed the product from their network.

Bluecat networks has a DNS/DHCP appliance - is there any interest in having them do a presentation. There as no response from the group.

Minutes were approved.

Apple just did a security presentation at OSU that we might want to consider for here.

Meeting was adjourned.