OARtech
12/13/2006

Attendance:
Denison University - Teresa Beamer
Ohio Northern University - Bob Beer
Clark State Community College - Bill Blake, Shane Bucher, Angie Davis, Steve Hurley, Chris Bunner, Chris Scanlon, Scott DeJane
CWRU - Eric Chan
Hocking College - Ben Dalton
Oberlin College - Cal Frye
University of Northwestern Ohio - Greg Gross
University of Akron - Deb Keller, Deb White
Sinclair Community College - Scott McCollum
Shawnee State University - Mike Pinson
University of Rio Grand - Kingsley Meyer
Wright State - Shane DeWalt, Patricia Vendt
Wittenberg - Scott Powell
Ohio Learning Network - Cable Green
BGSU - Mike Smith
Oarnet - Nancy Drugan Koehler, Dana Rogers, TJ Sandors, Paul Schopis, Mary Ann Zbydnowski

OARnet update
Paul Schopis

Arrived late to meeting so the minutes begin after first presentation started.

Partners
K-12 ITC - have about half the point connected
I2 and NLR - Paul is chairing the Newnet technical Advisory Committee. Both networks will be around for a wile. Oarnet will continue to engage both networks and get the best possible offerings for Ohio. I2 and NLR have very different business models. 2 Cleveland sites are already members of NLR. NLR connections will be in Chicago, and I2 in Cleveland.

PacketNet is functional as is the first wave of I2 Newnet. Oarnet is trying to get in the first wave of Newnet by February with connections in Cleveland. Interstate and Inter-Ron collaborations that provides natural extensions to move beyond the normal borders. One ideal opportunity is for TFN/Oarnet to connect to the OMNIpop. This gives Oarnet peering opportunities with CIC RON and the regional networks in the surrounding states. MERIT has approached Oarnet to connect in Chicago since they are looking to use Oarnet to get to Pittsburgh Super Computer Center. They share cost of the fiber and equipment is at an incremental cost. OSC would like to expand collaborations with Pittsburgh Super Computer Center and is working with PSC to provide connections for them to help in bringing in to CIC as well as Oarnet connections. NYSERNET (New York) would like to work with Oarnet to get collaborations with other super computing centers and is kind of developing into an adhoc OMNIpop east. Oarnet is being looked at as model for other regional nets that are coming up throughout the nation.

What was the I2 meeting like last week? The meeting was more civil given the current relations between NLR and I2.

Case Western is now on NLR. They are seeing very little traffic from it at this time. They had some issues with sending traffic via NLR and return traffic coming back via I2. Battelle is looking at purchasing NLR. There was some discussion on the issues between I2 and NLR and how the regional's and their peering relationships affect both the organizations.

CALEA Update
Paul Schopis

Slides are available on the web site:
http://www.osc.edu/oarnet/oartech/presentations.shtml

Prime Directive: At the end of the day, you are responsible and you should engage your legal counsel in the discussion since if the FBI says you have to comply, your legal counsel is prepared to argue their stance.

Original act was passed in 1994 and allowed law enforcement to gain intelligence in a lawful manner from the telecommunications carriers. In May 2006, there was a memorandum opinion and order that the act applies to Internet, VoIP, and cellular services. There are basically 2 parts - You have to have an operation plan by Feb 2007 that includes who does what and how you would comply, then you must have technical compliance by May 14, 2007.

The problem with the May 14th date is that they can't give specifics about what they really want or what compliance really means.

Who is affected? There were several source of confusion. There were 2 footnotes - 74 and 100. Under Footnote 74 if you are multi-homed you must be compliant. Footnote 100 says that if the private networks are internet connected with a public network then you are required to comply.

If you are required to comply, it is best for you to give it to your counsel upon receipt of a warrant or court order to determine the warrant's requirements. Engage the point of contact that only with the staff required servicing the warrant. You are required to give them only the information requested as you have to protect the privacy of the parties not involved in the warrant. You cannot just give a dump of all the data.

What they want is the call identifying information within 8 seconds of the receipt of the message at least 95% of the time and time stamped to an accuracy of 200 msec. You are not supposed to even look at the data. This is the ugliest scenario. If they ask for dialing or signaling info then netflow may be enough for dialing, routing, addressing, or signaling information transmitted by an instrument, or facility. Trap and trace captures the originating number, routing, and addressing, but does not include the contents of any communication.

This is a widely held belief that campuses are immune is predicated that the network meets the requirement of a private network. 2 scenarios can trump this: Public access to facilities (public systems in libraries) or if the upstream vendor cannot meet the request for valid technical reasons. If a law enforcement agency (LEA) comes to Oarnet with user id, name, jack, etc..., Oarnet does not have access to the information. So Oarnet would have to send the request downstream. The warrant can come to the individual campuses.

Paul will post the original legislation on the web site.

A good way to proceed is the identify the people that would work with Oarnet if an warrant is served and how you would go about working with the ISP.

It was suggested that we have someone from the Attorney General's office and/or the FBI come to an OARtech meeting and talk about the issues. Another suggestions was having an on-line session via OLN with representation from AG, FBI, Oarnet, and OSU legal counsel.

There are some instances that system admins are required to report proactively and not wait for a warrant. These should also be reviewed.

The FBI does understand that they need to be as close to the handset as possible to get the information they need. They cannot mandate the

way you provide the information as long as you can provide it in the requested format.

Paul worked out an idea that would allow you to comply (see slides for diagrams). Forwarding is based on source IP for outgoing and destination for inbound packets. The router sends this to the mediation Box. If the campus switch could do forwarding based on source MAC or could tag data for router to process it could forward with the IP or send to an MPLS tunnel for a label. Mediate box function receives the packet and duplicates it, wraps the original in a new packet to forward to the LEA and sends a copy to the gateway router. For reverse path you need to return to edge router in the vlan, MPLS or some other tagging mechanisms to prevent looping.

Vendors?
There are vendors trying to send a trusted third party service (APEGY) and they can handle both the technical and the legal issues that come up. They are targeting campuses more that regionals. Cisco says they are coming up with code that will have CALEA compliance built in.

Important documents:
www.askcalea.net
www.fcc.gov
www.atis.org
www.educause.edu

There is an RFC 3924 which is a standard for intercepting information. So there is a standard for intercepting info.

MERIT has some overview information; will Oarnet be distributing some of this information with templates and recommendations?

Motion and second to establish an OARtech committee to work with the Osteer CALEA committee on the technical issues with CALEA compliance. Motion was passed.
Shane Dewalt (Wright State) volunteered for the committee, Kurt Eckhart, Ransel Yoho (pending approval), Mike Pinson (Shawnee State), Eric Chan (Case Western), Cal Frye (Oberlin), Paul Schopis will appoint someone from Oarnet to the committee. Paul will also help with exchanging communications.

Lunch

Sophos
Carl St. John (Versatile), Brian Richwine and Beth Jones (via teleconference)
Slides are available on the web site:
http://www.osc.edu/oarnet/oartech/presentations.shtml

They will be scheduling a web event in January. Drop a business card in the box and they will let you know about the event. They will also draw a card for an Ipod.

Sophos is the 4th largest player in the anti-spam, anti-virus market.

Changes in the threat landscape: the threats are now more profit oriented.

Threat numbers: 3000 new malicious software threats per month. In November was over 7000. 300% rise in spam in May 2006. They are constantly developing more threats to get control of machines to do what they want them to do.

The profile of the virus writers is changing. It used to be ego centric. Now it is more profit oriented and have seen some extortion attempts (they delete your data unless you send them money or buy off they site). Legal enforcement has to be involved.

Most of the Trojans have spy ware components. Now we have MalPacker

and Mal/Banc behavioral genotypes. They don't want to draw attention to themselves and there is strong evidence that they 'test' first and are targeting small institutions. They hide themselves with self updating and packing techniques. There are now malware kits for sale.

Changing face of spam
They are seeing an increase in the image-only spam that is widely used for stock pump and dump and now are being used for other types. Spammers are registering new URLs every 5 minutes and abusing the free mail sites and registers. The landscape is changing so that virus writing gangs and spammers were separate, but now they are starting to merge and help each other. Dec 2005 68% Trojans in May 2006 84% Trojans.

How threat is deployed:
Email seed-list with message sent to the seed list. It will point to a web site that was probably purchase with a stolen credit card. The end users click on the link and it automatically downloads their payload after shutting down the anti-virus software. These could include Trojans, Botnets (create a zombie network to harvest information, etc controlled by a single server), and rootkits. Rootkits in and of themselves is not malicious, but what it is hiding usually is. Rootkits are used by the attacker to maintain access and hide the activity from the system administrator. The rootkit gets inserted between the application and the system so that it can do the responses to the application allowing it to gather information and hide itself.

Malware authors are using newer or different tactics to try and maintain their element of surprise using different techniques to keep the infection ratio up. The reason obfuscation techniques work is because AV is reactionary. Obfuscation techniques include, browser help objects, because they sniff http traffic and is the core of Adware. As you try to get rid of it, it keeps spawning itself. They are persistent, you termination and it respawns itself. Exploit usage is most commonly using vulnerabilities in unpatched windows. The point being that one vulnerability can install multiple Trojans and/or backdoors by finding one exploit. ADODB - all you have to do is view the website and it installs the down loaders, and backdoors.

Games - MMORPGs are massive multiplayer online role-playing games that contain phishing, keylogging, etc... The mechanism is they steal the login credentials, they transfer items within games and then sell them for real cash. The games allow creation of items and then the infections is used to affect the other characters and aspects of the games.

SophoLabs is an engineering group that works for Sophos and they have overlapping support times. This helps them to keep on top of outbreaks. They look at the viruses and spam and send out the updates, alerts and information. Anti-virus updates are 4-6 times a day with the capability of pushing out additional updates as necessary. Anti-spam updates are run every 5 minutes. They provide virus alerts via email, Zombie alerts (you can ask them to check the network for spam zombies), and phishing alerts (notify your company if they see a phishing email using your company's name).

They use honeypots and other ways the intercepting the sample viruses. This info is analyzed by SophosLabs who write classification, detection, and removal scripts. They test the scripts and then publish the scripts. To help them find seeding campaigns they detect the initial variants then spot the family type of infection and then install the scripts to identify the entire family type of infection. Thus being a more pro-active protection of new malware.

What they expect to see:
More of the same stealing and phishing and some are trying to legally

harvest the data. The volume will increase. They are trying to move away from the one signature per threat. They are trying to use a genotype technology that they introduced in 2004 that determines the characteristics and correlate detect the infections including identifying suspicious behavior.

MS Vista
Sophos didn't have any issues running on vista. They are using outbound firewall filtering. They talked a little about PatchGuard, and other miscellaneous utilities.

The threats are becoming more campaigns and more professional and coordinated, and persistent. This does not mean the code is better, in some cases it is quite sloppy. It is financially motivated.

www.solphos.com
NASales@sophos.com
Sales@sophos.com

We indicated that cross platform anti-virus support of Sophos very important to those of use currently using it.

Discussed some issues on Sophos appliance and what is available.

You can see the chronological list of the viruses and who found them:
http://www.secunia.com

Contact for further information
Brian Richwine
National Account Manager
Sophos, Inc.
3 Van de Graaff Drive
2nd floor
Burlington, MA 01803
Cell: 740-508-272-3491
Direct: 781-494-5922
Brian.richwine@sophos.com

Meeting was adjourned at 2:25