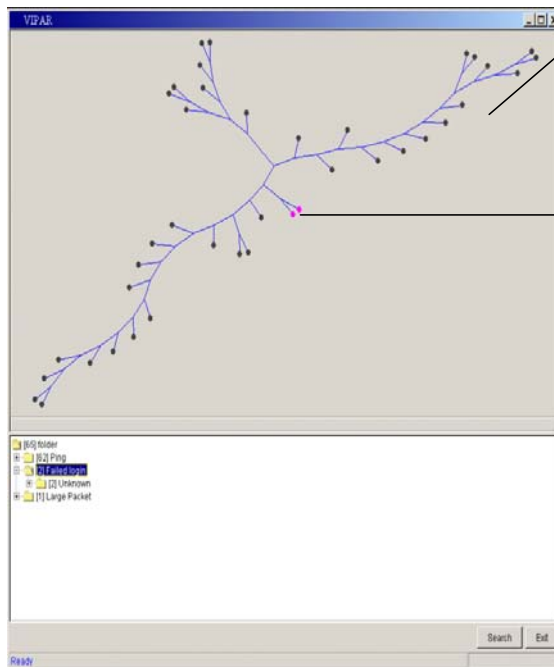


CIPHER

Counterintelligence Penetration Hazard Evaluation and Recognition

A great deal of very sensitive information resides on a very wide collection of computer networks. This information ranges from personal credit card information to nuclear weapons design. Typically this information is heavily protected, and likewise, highly sought after by various illicit groups. These groups use a wide variety of means to gain access to this sensitive data. These means can be broadly classified into three areas, unsophisticated, semi-sophisticated, and highly sophisticated attacks. The problem posed by this unsophisticated type of attack is well in hand. The semi-sophisticated attack can often be identified through a wide range of anomaly detection techniques. However, the sophisticated attackers understand how intrusion detection and firewall software work, and use methods that will not raise concerns in either system. Currently, there is no way to prevent this type of “low and slow” attack, or to even recognize when it occurs, until now.

Cipher analyzes activity against valuable organizational assets, not merely at network packet statistics. We have demonstrated CIPHER using 1 million suspect records that occur daily on the ORNL networks.



45 “low and slow” pings from:
 –Czech Republic, Austria, Hungary, Latvia, France, Chile, and Canada.

2 attacks on nanotechnology scientists

Source IP: 200.10.225.87 ncache07.terra.cl

Date/Time	Source Port	Destination IP	Destination Hostname	PI Name	Research Area	Destination Port	Length	Filter
0703 14:14:30		128.219.49.130	3Q/32 CT ORNL 0009	Hidden	Chemical and Material Science on Nanotechnology Surface Phenomena Fluorines	4545	455	Beta-000014 BETA WEB - 403 Forbidden
0703 14:29:30		128.219.49.130	3Q/32 CT ORNL 0009	Hidden	Chemical and Material Science on Nanotechnology Surface Phenomena Fluorines	4532	455	Beta-000014 BETA WEB - 403 Forbidden
0703 14:58:30		128.219.49.130	3Q/32 CT ORNL 0009	Hidden	Chemical and Material Science on Nanotechnology Surface Phenomena Fluorines	4554	455	Beta-000014 BETA WEB - 403 Forbidden
0703 15:11:30		128.219.49.130	3Q/32 CT ORNL 0009	Hidden	Chemical and Material Science on Nanotechnology Surface Phenomena Fluorines	4700	455	Beta-000014 BETA WEB - 403 Forbidden
0703 15:21:30		128.219.49.130	3Q/32 CT ORNL 0009	Hidden	Chemical and Material Science on Nanotechnology Surface Phenomena Fluorines	4554	455	Beta-000014 BETA WEB - 403 Forbidden
0703 16:17:30		128.219.49.130	3Q/32 CT ORNL 0009	Hidden	Chemical and Material Science on Nanotechnology Surface Phenomena Fluorines	1709	455	Beta-000014 BETA WEB - 403 Forbidden
0703 16:41:30		128.219.49.130	3Q/32 CT ORNL 0009	Hidden	Chemical and Material Science on Nanotechnology Surface Phenomena Fluorines	2130	455	Beta-000014 BETA WEB - 403 Forbidden
0703 17:06:30		128.219.49.130	3Q/32 CT ORNL 0009	Hidden	Chemical and Material Science on Nanotechnology Surface Phenomena Fluorines	3225	455	Beta-000014 BETA WEB - 403 Forbidden
0703 17:27:30		128.219.49.130	3Q/32 CT ORNL 0009	Hidden	Chemical and Material Science on Nanotechnology Surface Phenomena Fluorines	3575	455	Beta-000014 BETA WEB - 403 Forbidden

CIPHER allows us to quickly finding potential “low and slow” intrusion attacks from sophisticated attackers.

POC: Thomas E. Potok, Ph.D.
 Oak Ridge National Laboratory
 P.O. Box 2008, Oak Ridge, TN 37831-6415
 Phone/Email: 865-574-0834/potokte@ornl.gov